User Guide

ORiNOCO AP-4000 Series Access Points
User Guide

PROXIM WIRELESS NETWORKS

Copyright

© 2005 Proxim Corporation. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Corporation.

Trademarks

ORiNOCO is a registered trademark, and Proxim, and the Proxim logo are trademarks of Proxim Corporation.

Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Ekahau is a trademark of Ekahau, Inc.

HyperTerminal is a registered trademark of HilGraeve, Incorporated.

Microsoft and Windows are a registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

SolarWinds is a registered trademark of SolarWinds.net.

All other trademarks mentioned herein are the property of their respective owners.

OpenSSL License Note

This product contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and that is subject to the following copyright and conditions:

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to refer to, endorse, or promote the products or for any other purpose related to the products without prior written permission. For written permission, please contact openssl-core@openssl.org.

This software is provided by the OpenSSL Project "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the OpenSSL Project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

ORiNOCO AP-4000 Series User Guide

Software v3.1
P/N 71124 August 2005

Contents

1 Introduction 9
Products Covered in this User Guide 9
Document Conventions 9
Introduction to Wireless Networking 10
Mesh Networking (AP-4000M/4900M Only) 11
Mesh Network Convergence 11
Mesh Network Configuration 13
Guidelines for Roaming 14
IEEE 802.11 Specifications 15
Management and Monitoring Capabilities 15
HTTP/HTTPS Interface 15
Command Line Interface 15
SNMP Management 16
SSH (Secure Shell) Management 17
2 Installation and Initialization 18
AP-4000 Series Hardware Description 18
Overview 18
Antennas 19
Active Ethernet 20
LED Indicators 21
Prerequisites 22
General Prerequisites 22
Mesh Prerequisites 23
Product Package 24
System Requirements 24
Hardware Installation 25
Required Materials 25
Cabling the AP-4000/4000M/4900M 25
Installing the Security Cover 26
Mounting the AP-4000/4000M/4900M 26
Installing External Antennas 28
Installing the AP in a Plenum 29
Initialization 31
Using ScanTool 31
Logging In 33
Using the Setup Wizard 35
Installing the Software 37
Related Topics 40

3 System Status 41

4 Advanced Configuration 42

System 44
Dynamic DNS Support 44
Network 46
IP Configuration 46
DHCP Server 47
DHCP Relay Agent 49
Link Integrity 50
SNTP (Simple Network Time Protocol) 51
Interfaces 54
Operational Mode 54
Wireless-A (802.11a Radio) and Wireless-B (802.11b/g Radio) 57
Ethernet 64
Mesh (AP-4000M/AP-4900M Only) 66
Management 68
Passwords 68
IP Access Table 69
Services 69
Automatic Configuration (AutoConfig) 75
Hardware Configuration Reset (CHRD) 77
Filtering 80
Ethernet Protocol 80
Static MAC 80
Advanced 83
TCP/UDP Port 83
Alarms 85
Groups 85
Syslog 90
Rogue Scan 93
Bridge 97
Spanning Tree 97
Storm Threshold 98
Intra BSS 99
Packet Forwarding 99
QoS 100
Wireless Multimedia Extensions (WME)/Quality of Service (QoS) 100
Priority Mapping 102
Enhanced Distributed Channel Access (EDCA) 103
Radius Profiles 106
RADIUS Servers per Authentication Mode and per VLAN 106

Configuring Radius Profiles . . . 107
MAC Access Control Via RADIUS Authentication . . . 110
802.1x Authentication using RADIUS . . . 110
RADIUS Accounting . . . 110
SSID/VLAN/Security . . . 113
VLAN Overview . . . 113
Management VLAN . . . 115
Security Profile . . . 116
MAC Access . . . 123
Wireless-A or Wireless-B . . . 123
Broadcast SSID and Closed System . . . 128

5 Monitoring . . . 129

Version . . . 130
ICMP . . . 131
IP/ARP Table . . . 131
Learn Table . . . 132
IAPP . . . 132
RADIUS . . . 133
Interfaces . . . 134
Station Statistics . . . 137
Mesh Statistics . . . 138

6 Commands . . . 139

Introduction to File Transfer via TFTP or HTTP . . . 139
TFTP File Transfer Guidelines . . . 140
HTTP File Transfer Guidelines . . . 140
Image Error Checking During File Transfer . . . 140
Update AP . . . 141
Update AP via TFTP . . . 141
Update AP via HTTP . . . 142
Retrieve File . . . 143
Retrieve File via TFTP . . . 143
Retrieve File via HTTP . . . 144
Reboot . . . 146
Reset . . . 146
Help Link . . . 147

7 Troubleshooting . . . 148

Troubleshooting Concepts . . . 148
Symptoms and Solutions . . . 148

Connectivity Issues . . . 148
Basic Software Setup and Configuration Problems . . . 149
Client Connection Problems . . . 150
VLAN Operation Issues . . . 151
Active Ethernet (AE) . . . 151
Recovery Procedures . . . 152
Reset to Factory Default Procedure . . . 152
Forced Reload Procedure . . . 152
Setting IP Address using Serial Port . . . 155
Related Applications . . . 156
RADIUS Authentication Server . . . 156
TFTP Server . . . 157

A Command Line Interface (CLI) . . . 158

General Notes . . . 158
Prerequisite Skills and Knowledge . . . 158
Notation Conventions . . . 158
Important Terminology . . . 158
Navigation and Special Keys . . . 159
CLI Error Messages . . . 159
Command Line Interface (CLI) Variations . . . 160
Bootloader CLI . . . 160
CLI Command Types . . . 161
Operational CLI Commands . . . 161
Parameter Control Commands . . . 165
Using Tables and Strings . . . 169
Working with Tables . . . 169
Using Strings . . . 169
Configuring the AP using CLI commands . . . 170
Log into the AP using HyperTerminal . . . 170
Log into the AP using Telnet . . . 170
Set Basic Configuration Parameters using CLI Commands . . . 170
Other Network Settings . . . 175
CLI Monitoring Parameters . . . 184
Parameter Tables . . . 184
System Parameters . . . 187
Network Parameters . . . 188
Interface Parameters . . . 191
Management Parameters . . . 197
Filtering Parameters . . . 202
Alarms Parameters . . . 204

Bridge Parameters . . . 206
RADIUS Parameters . . . 208
Security Parameters . . . 209
VLAN/SSID Parameters . . . 211
Other Parameters . . . 211
Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters . . . 211
CLI Batch File . . . 214
Auto Configuration and the CLI Batch File . . . 214
CLI Batch File Format and Syntax . . . 214
Reboot Behavior . . . 215

B ASCII Character Chart . . . 216

C Specifications . . . 217
Software Features . . . 217
Number of Stations per BSS . . . 217
Management Functions . . . 217
Advanced Bridging Functions . . . 218
Medium Access Control (MAC) Functions . . . 218
Security Functions . . . 218
Network Functions . . . 219
Hardware Specifications . . . 220
Physical Specifications . . . 220
Electrical Specifications . . . 220
Environmental Specifications . . . 220
Ethernet Interface . . . 220
Serial Port Interface . . . 220
Active Ethernet Interface . . . 220
Available Channels . . . 221
AP-4000/4000M Channels . . . 221
AP-4900M Channels . . . 222

D Technical Support . . . 224
Online Support . . . 224
Telephone Support . . . 225

E Statement of Warranty . . . 226
Warranty Coverage . . . 226
Repair or Replacement . . . 226
Limitations of Warranty . . . 226
Support Procedures . . . 226
Other Information . . . 227
Search Knowledgebase . . . 227

Ask a Question or Open an Issue 227
Other Adapter Cards 227

F Regulatory Compliance 228

Safety Information (USA, Canada, & European Union) 230
Federal Communications Commission (FCC) (AP-4000/4000M) 231
Warnings 232
Caution: Exposure to Radio Frequency Radiation 232
Modifications 232
Industry Canada (IC) (AP-4000/4000M only) 233
European Union (AP-4000/4000M only) 234
Regulatory Compliance Certifications Summary (AP-4000/4000M) 235
Regulatory Compliance Certifications Summary (AP-4900M) 235

1 Introduction

This chapter contains information on the following:

- Products Covered in this User Guide
- Document Conventions
- Introduction to Wireless Networking
- Mesh Networking (AP-4000M/4900M Only)
- Guidelines for Roaming
- IEEE 802.11 Specifications
- Management and Monitoring Capabilities

Products Covered in this User Guide

This User Guide details functionality of the AP-4000 Series Access Points, consisting of the following:

Product	Description
AP-4000	Tri-mode AP that supports: • 802.11b, 802.11g, or 802.11a clients simultaneously The AP-4000 can be converted to an AP-4000M using Proxim's Mesh Software Kit.
AP-4000M	Tri-mode AP that supports: • 802.11b, 802.11g, or 802.11a clients simultaneously • Mesh networking
AP-49000M	Tri-mode AP that supports: • 802.11b, 802.11g, or 802.11a clients simultaneously • Mesh networking • Operation in the 4.9 GHz Public Safety band

Document Conventions

- **AP** refers to an AP-4000, AP-4000M, or AP-4900M Access Point.
- **AP Series** refers to the AP-4000, AP-4000M and AP-4900M Access Points.

  NOTE: *Unless otherwise noted, screen captures in this User Guide are from the AP-4000.*
- **802.11** is used to describe features that apply to the 802.11a, 802.11b, and 802.11g wireless standards.
- Blue underlined text indicates a link to a topic or Web address. If you are viewing this documentation on your computer, click the blue text to jump to the linked item.
- Text enclosed within triangle brackets, < >, should be replaced with a user-defined value.
- The following special notations are used:

  NOTE: *A note contains important information that helps you make better use of the AP or your computer.*

  CAUTION: *A Caution indicates potential damage to hardware or loss of data.*

  WARNING: A Warning indicates imminent danger to hardware or loss of data.

Introduction to Wireless Networking

An Access Point extends the capability of an existing Ethernet network to devices on a wireless network. Wireless devices can connect to a single Access Point, or they can move between multiple Access Points located within the same vicinity. As wireless clients move from one coverage cell to another, they maintain network connectivity.

In a typical network environment (see Figure 1-1), the AP functions as a wireless network access point to data and voice networks. An AP network provides:

- Seamless client roaming for both data and voice (VoIP)
- Easy installation and operation
- Over-the-air encryption of data
- High speed network links

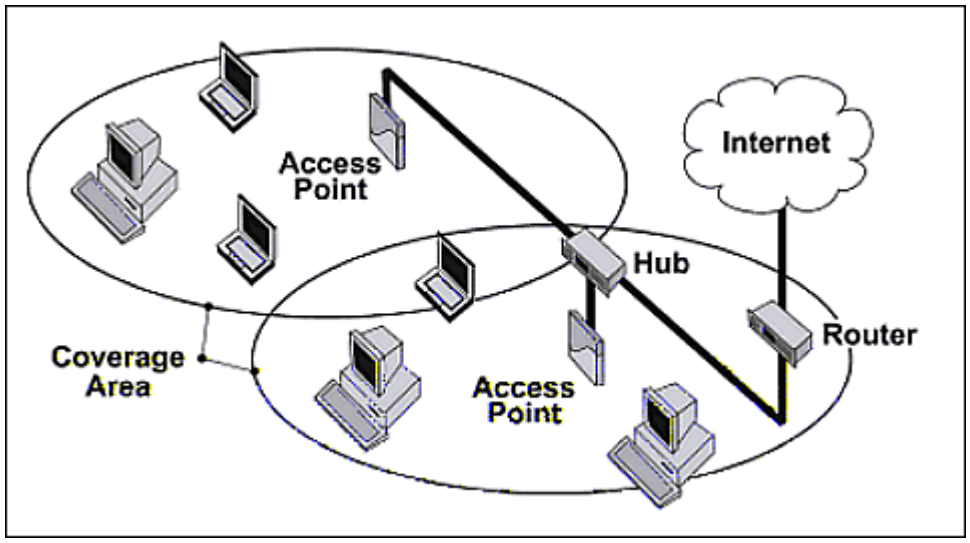


Figure 1-1 Typical Wireless Network Access Infrastructure

Mesh Networking (AP-4000M/4900M Only)

Using the ORiNOCO Mesh Creation Protocol (OMCP), The AP-4000M and AP-4900M support structured Mesh networking. For information on converting an AP-4000 into an AP-4000M to enable Mesh functionality, see Mesh Software Kit.

In a mesh network, access points use their wireless interface as a backhaul to the rest of the network. Access points connected directly to the wired infrastructure are called “portals;” mesh access points relay packets to other mesh access points to reach the portal, dynamically determining the best route over multiple “hops.”

Mesh networks are self-configuring (a mesh access point will scan for other mesh access points periodically and choose the best path to the portal) and self-healing (the network will reconfigure data paths if an AP or link fails or becomes inactive).

Mesh Network Convergence

Mesh networks are formed when mesh APs on the same channel have the identical Mesh SSIDs, security settings, and management VLAN IDs when VLAN is enabled. As these Mesh APs come online, they discover and set up links with each other to form the Mesh network.

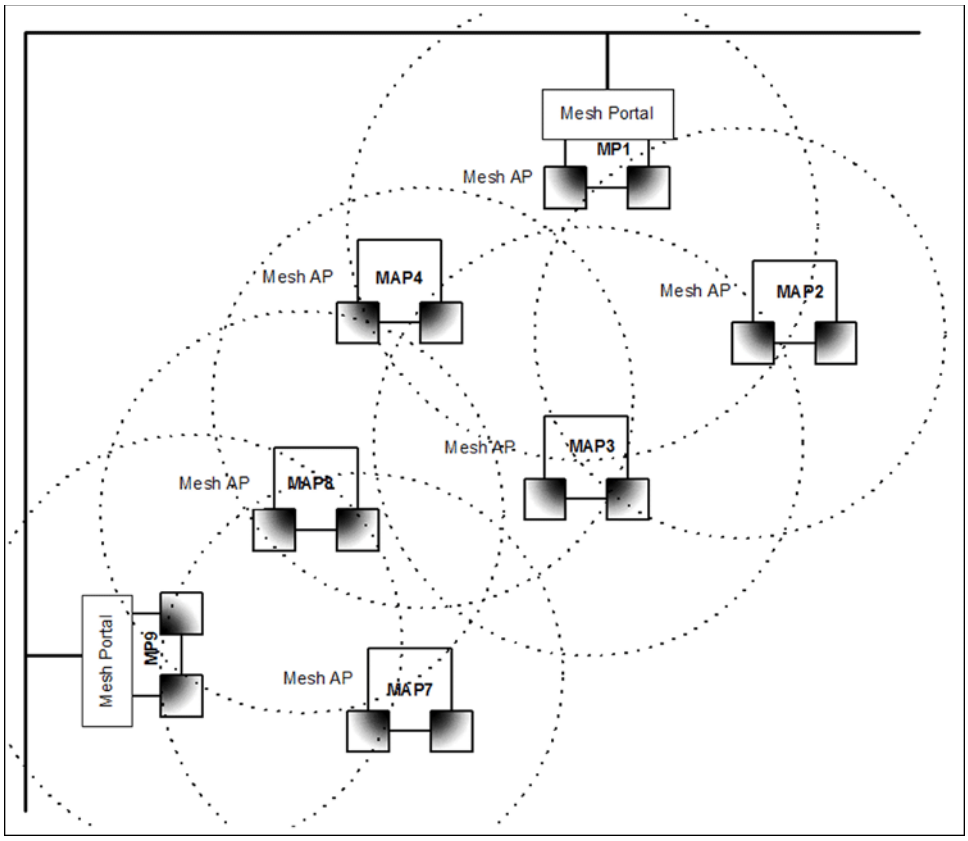


Figure 1-2 Mesh Startup Topology Example – Step 1

In Figure 1-2, MP1 and MP9 are APs configured as Mesh portals, each on a different channel. When they are up and running, they will transmit beacons with a Mesh information element (IE) containing a Mesh SSID, and respond to probe requests that contain Mesh IEs with the same Mesh SSID.

To find Mesh connections, Mesh AP (MAP) 2 through 8 will scan all allowed channels, either actively or passively. In active scanning, the MAP sends a broadcast probe request; in passive scanning, the MAP listens for beacons. Active scanning is used in regulatory domains that do not use Dynamic Frequency Selection (DFS); passive scanning is used in DFS-controlled regulatory domains (see Dynamic Frequency Selection/Radar Detection (DFS/RD)). As other Mesh APs

are discovered, MAP2 through MAP8 will build a neighbor table from the beacons and probe responses they receive. The neighbor table contains three kinds of links:

- Active: Link with a mesh neighbor that has gone through association and authentication, and the port is open.
- Connected: Link with a mesh neighbor that has gone through association and authentication, but the port is closed.
- Disconnected: Possible link to a mesh neighbor that has not gone through association and authentication.

From the neighbor table, MAP2 through MAP8 will select the best possible connection to the backbone network. This connection is the active link. If a link to the backbone on a different channel is significantly better than any on the current channel, then MAP2 through MAP8 will switch to a new channel and join the Mesh network on that channel.

In Figure 1-2 through Figure 1-4, the circles approximately indicate the range of the respective Mesh radios. As shown in these figures, MAP2 and MAP4 will discover Mesh Portal (MP) 1, and MAP7 and MAP8 will discover MP9. MAP3 is also within reach of MAP2 and MAP4, but they will not allow MAP3 to connect until they have established a Mesh link to the Mesh Portal.

Assume that links are established as shown in Figure 1-3. Solid lines indicate established links.

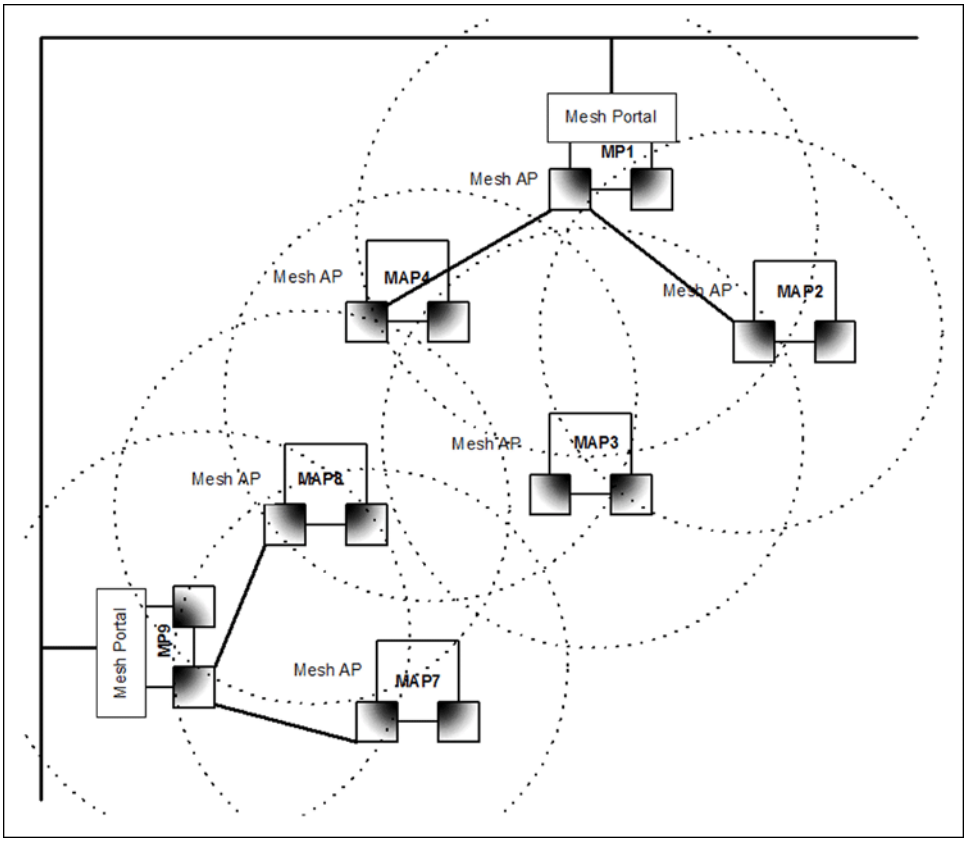


Figure 1-3 Mesh Startup Topology Example – Step 2

After the first Mesh links are formed, MAP2,4,7 and 8 will add the Mesh IE to their beacon and respond to probe requests with a Mesh IE containing the same Mesh SSID and security settings. Eventually MAP 3 will find both MAP2 and 4 and will setup a Mesh link with the one with the best path to the portal, say MAP2. Optimal paths are chosen based on the number of hops to the portal, RSSI (relative signal strength), and medium (air) utilization.

Once MAP4 has established a path to the Mesh portal, MAP 3 will also establish a Mesh link with MAP4, but that connection will remain inactive. It will only be used as a possible alternative link. Similarly, the link between MAP3 and MAP4 is an alternative uplink for MAP3, and at the same time an alternative uplink for MAP4. If for some reason the link

from MAP4 to MP1 fails, MAP4 can still reach the backbone via MAP3 and MAP2. The same goes for other MAPs that discover each other.

After a short while, the network in this example will look like Figure 1-4, where solid lines indicate active Mesh links and dotted lines indicate established but inactive Mesh links.

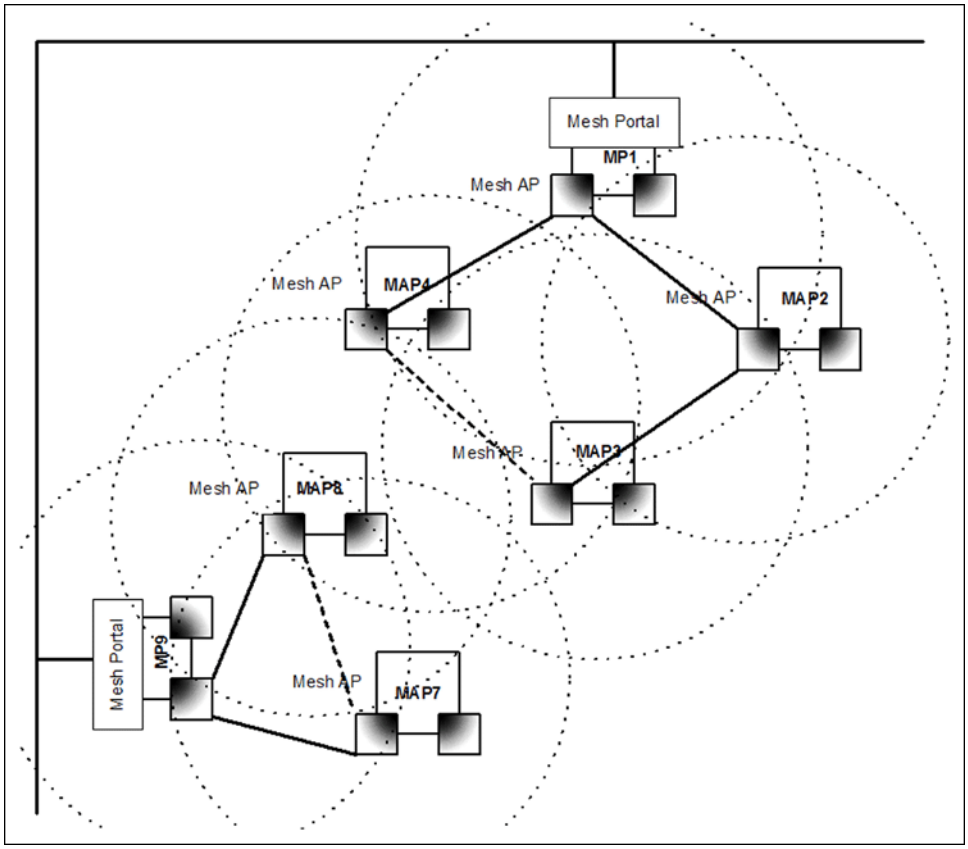


Figure 1-4 Mesh Startup Topology Example – Step 3

In this example, if MAP8 loses the Mesh link to MP1, MAP8 will immediately activate the Mesh link to MAP7. If the link to MAP7 has a higher path cost than a possible link to MAP4, which has the same Mesh SSID and security mode but is on a different channel, then MAP7 may decide to switch channels and establish and activate a link to MAP4.

Mesh Network Configuration

In the AP-4000M/4900M, either of the wireless interfaces may be configured for Mesh functionality, with the following considerations in mind:

- To form or join a Mesh network, Mesh APs must have identical Mesh SSIDs and security modes (None or AES).
- All Mesh APs within a network must be on the same channel. The channel used by the Mesh portal will determine the channel used by the entire mesh network.
- Mesh APs must have static IP addresses, as the DHCP client will not function on wireless interfaces.
- On Mesh APs, Mesh and WDS functionality cannot co-exist on the same wireless interface. Mesh and WDS can co-exist on Mesh Portals.
- The maximum number of links in the mesh network is 6. Proxim recommends that administrators configure their Mesh network to allow between 20-30 access points per portal for an average per-client throughput of 300-500 Kbps. This recommendation is based on the following assumptions:

  - 18 Mbps throughput is available at the portal (max is 25 Mbps, but APs will back off as distance between them increases).
  - 20 wireless clients are supported per AP.
  - Average utilization (time that a client is actually transferring data) is 10%.

  If the conditions on your network are different than the assumptions above, then the maximum number of APs should be adjusted accordingly.

  NOTE: *Clients whose traffic must traverse multiple hops in order to reach the portal will have lower throughput than clients whose traffic traverses fewer hops.*

- Although this solution is designed to be flexible and have a short convergence time after a topology change, it is not recommended for high-speed roaming or a highly dynamic environment. Typical roaming times are as follows:
  - When switching between portals on the same channel: >50 ms
  - When switching between portals on different channels: >500 ms

  These times apply whether the Mesh AP is mobile or stationary.
- The Mesh network assumes that the uplink to the backbone will be provided by Mesh only. To avoid loops, the administrator should not configure alternate links to the backbone through Ethernet or WDS connections.
- Mesh APs will detect and avoid loops caused by Mesh links; similarly, Spanning Tree will detect and avoid loops caused by WDS and wired links. However, neither Mesh APs nor Spanning Tree will detect loops caused by a mixture of Mesh and WDS/wired links. Administrators should avoid any such scenario while deploying Mesh.
- When VLAN is enabled, all APs in a Mesh network must have the same Management VLAN ID.

For information on configuring Mesh using the HTTP interface, see Mesh (AP-4000M/AP-4900M Only). For information on configuring Mesh using the Command Line Interface (CLI), see Mesh Network Parameters in the Command Line Interface chapter.

Guidelines for Roaming

- Typical voice network cell coverages vary based on environment. Proxim recommends having a site survey done professionally to ensure optimal performance. For professional site surveyors, Ekahau™ Site Survey software is included in the Xtras folder of the Installation CD.
- An AP can only communicate with client devices that support its wireless standard.
- All Access Points must have the same Network Name to support client roaming.
- All workstations with an 802.11 client adapter installed must use either a Network Name of “any” or the same Network Name as the Access Points that they will roam between. If an AP has Closed System enabled, a client must have the same Network Name as the Access Point to communicate (see Broadcast SSID and Closed System).
- All Access Points and clients must have matching security settings to communicate.
- The Access Points’ cells should overlap to ensure that there are no gaps in coverage and to ensure that the roaming client will always have a connection available. To ensure optimal AP placement, Proxim recommends having a professional site survey done. To facilitate the automation of this placement, site surveyors may use the Ekahau™ Site Survey software included in the Xtras folder of the Installation CD.
- An 802.11a or 802.11b/g AP operates at faster data rates than the 802.11b AP. 802.11a and 802.11g products operate at speeds of up to 54 Mbits/sec; 802.11b products operate at speeds of up to 11 Mbits/sec.
- All Access Points in the same vicinity should use a unique, independent channel. By default, the AP automatically scans for available channels during boot-up but you can also set the channel manually (see Interfaces for details).
- Access Points that use the same channel should be installed as far away from each other as possible to reduce potential interference.
- If a Mesh AP switches to a new uplink, by default it will send a deauthentication message to clients connected to it. Administrators can prevent the sending of this message by disabling the “sendclientdeathmessage” parameter in the Command Line Interface. See Mesh Network Parameters in the Command Line Interface (CLI) chapter.

- In countries that require passive scanning for Mesh, the roam time may be higher.
- When an AP-4000M/4900M is mounted in a vehicle and is being used in a Mesh network, there will be limited connectivity when the vehicle is moving.

IEEE 802.11 Specifications

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11 standard operate at a data rate of either 1 or 2 Megabits per second (Mbits/sec).

In 1999, the IEEE modified the 802.11 standard to support direct sequence devices that can operate at speeds of up to 11 Mbits/sec. The IEEE ratified this standard as **802.11b**. 802.11b devices are backwards compatible with 2.4 GHz 802.11 direct sequence devices (that operate at 1 or 2 Mbits/sec). Available Frequency Channels vary by regulatory domain and/or country. See Available Channels for details.

Also in 1999, the IEEE modified the 802.11 standard to support devices operating in the 5 GHz frequency band. This standard is referred to as **802.11a**. 802.11a devices are not compatible with 2.4 GHz 802.11 or 802.11b devices. 802.11a radios use a radio technology called Orthogonal Frequency Division Multiplexing (OFDM) to achieve data rates of up to 54 Mbits/sec. Available Frequency Channels vary by regulatory domain and/or country. See Available Channels for details.

In 2003, the IEEE introduced the **802.11g** standard. 802.11g devices operate in the 2.4 GHz frequency band using OFDM to achieve data rates of up to 54 Mbits/sec. In addition, 802.11g devices are backwards compatible with 802.11b devices. Available Frequency Channels vary by regulatory domain and/or country. See Available Channels for details.

Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage an AP on the network:

- HTTP/HTTPS Interface
- Command Line Interface
- SNMP Management
- SSH (Secure Shell) Management

HTTP/HTTPS Interface

The HTTP Interface (Web browser Interface) provides easy access to configuration settings and network statistics from any computer on the network. You can access the HTTP Interface over your LAN (switch, hub, etc.), over the Internet, or with a “crossover” Ethernet cable connected directly to your computer’s Ethernet Port.

HTTPS provides an HTTP connection over a Secure Socket Layer. HTTPS is one of three available secure management options on the AP; the other secure management options are SNMPv3 and SSH. Enabling HTTPS allows the user to access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate.

The AP comes pre-installed with all required SSL files: default certificate, private key and SSL Certificate Passphrase installed.

Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage an AP.

Users enter Command Statements, composed of CLI Commands and their associated parameters. Statements may be issued from the keyboard for real time control, or from scripts that automate configuration.

For example, when downloading a file, administrators enter the **download** CLI Command along with IP Address, file name, and file type parameters.

You access the CLI over a HyperTerminal serial connection or via Telnet. During initial configuration, you can use the CLI over a serial port connection to configure an Access Point's IP address. When accessing the CLI via Telnet, you can communicate with the Access Point from over your LAN (switch, hub, etc.), from over the Internet, or with a "crossover" Ethernet cable connected directly to your computer's Ethernet Port. See Command Line Interface (CLI) for more information on the CLI and for a list of CLI commands and parameters.

SNMP Management

In addition to the HTTP and the CLI interfaces, you can also manage and configure an AP using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program, like HP Openview or Castlerock's SNMPc. The AP supports several Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Ethernet-like MIB (RFC 1643)
- 802.11 MIB
- ORiNOCO Enterprise MIB

Proxim provides these MIB files on the CD-ROM included with each Access Point. You need to compile one or more of the above MIBs into your SNMP program's database before you can manage an Access Point using SNMP. See the documentation that came with your SNMP manager for instructions on how to compile MIBs.

The Enterprise MIB defines the read and read-write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. See the Enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word, Notepad, or WordPad.

SNMPv3 Secure Management

SNMPv3 is based on the existing SNMP framework, but addresses security requirements for device and network management.

The security threats addressed by Secure Management are:

- *Modification of information*: An entity could alter an in-transit message generated by an authorized entity in such a way as to effect unauthorized management operations, including the setting of object values. The essence of this threat is that an unauthorized entity could change any management parameter, including those related to configuration, operations, and accounting.
- *Masquerade*: Management operations that are not authorized for some entity may be attempted by that entity by assuming the identity of an authorized entity.
- *Message stream modification*: SNMP is designed to operate over a connectionless transport protocol. There is a threat that SNMP messages could be reordered, delayed, or replayed (duplicated) to effect unauthorized management operations. For example, a message to reboot a device could be copied and replayed later.
- *Disclosure*: An entity could observe exchanges between a manager and an agent and thereby could learn of notifiable events and the values of managed objects. For example, the observation of a set command that changes passwords would enable an attacker to learn the new passwords.

To address the security threats listed above, SNMPv3 provides the following when secure management is enabled:

- Authentication: Provides data integrity and data origin authentication.

- Privacy (a.k.a Encryption): Protects against disclosure of message payload.
- Access Control: Controls and authorizes access to managed objects.

The default SNMPv3 username is **administrator**, with SHA authentication, and DES privacy protocol.

SSH (Secure Shell) Management

You may securely also manage the AP using SSH (Secure Shell). The AP supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data.

The SSH server (AP) has ***host keys*** - a pair of asymmetric keys - a ***private key*** that resides on the AP and a ***public key*** that is distributed to clients that need to connect to the AP. As the client has knowledge of the server host keys, the client can verify that it is communicating with the correct SSH server.

NOTE: *The remainder of this guide describes how to configure an AP using the HTTP Web interface or the CLI interface. For information on how to manage devices using SNMP or SSH, see the documentation that came with your SNMP or SSH program. Also, see the MIB files for information on the parameters available via SNMP and SSH.*

2 Installation and Initialization

This chapter contains information on the following:

- AP-4000 Series Hardware Description
  - Overview
  - Antennas
  - Active Ethernet
  - LED Indicators
- Prerequisites
  - General Prerequisites
  - Mesh Prerequisites
- Product Package
- System Requirements
- Hardware Installation
- Initialization
  - Using ScanTool
  - Logging In
  - Using the Setup Wizard
  - Installing the Software
- Related Topics

AP-4000 Series Hardware Description

Overview

The AP-4000, AP-4000M, and AP-4900M are tri-mode APs that simultaneously support 802.11b, 802.11g, or 802.11a clients.

The AP-4000/4000M/4900M contains two embedded radios: one 802.11b/g radio and one 802.11a only radio. The 802.11a radio supports operation in 802.11a only mode in the AP-4000, and operation in either 802.11a only or 4.9 GHz Public Safety mode in the AP-4900M. 4.9 GHz Public Safety mode is for use in the licensed 4.9 GHz band; only users with licenses to operate in this band should access it.

The 802.11b/g radio supports the following operational modes:

- 802.11b only mode
- 802.11g only mode
- 802.11b/g mode
- 802.11g-wifi

NOTE: *802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.*

The AP-4000/4000M/4900M can be powered through either Active Ethernet (802.3af Power over Ethernet) or through an external DC power source using the power cord.

The AP-4000/4000M/4900M includes a a power jack, a 10/100 base-T Ethernet port, and an RS-232 serial data communication port. The AP includes an optional security cover that can be installed to protect against access to the power and LAN cables and to the reset and reload buttons. See Figure 2-1.

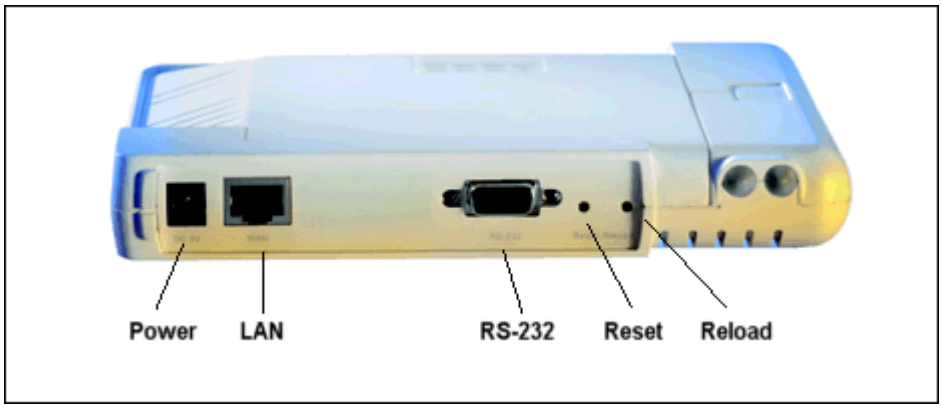


Figure 2-1 Rear Panel

The AP-4000/4000M/4900M has been designed to rest horizontally on a flat surface, but can be wall- or ceiling- mounted with the long axis vertical. The unit includes screw slots in the bottom plastic for mounting to a flat wall or ceiling.

Antennas

Each radio on the AP-4000/4000M/4900M employs two internal antennas for antenna diversity: one is vertically polarized, and the other is horizontally polarized to provide optimal spatial and polarization diversity. When the AP is hung on the wall of an office or building, the horizontally polarized antenna provides coverage for that particular floor level. The vertically polarized antenna provides spatial diversity for the horizontally polarized antenna in the event of an antenna null. In addition, the vertically polarized antenna provides some coverage above and below the current floor level. When the AP is mounted on the ceiling or sitting on a table, the effect is the same, but the roles of the two antennas switch.

The AP supports both receive and transmit diversity. When receiving, the AP chooses the antenna that recieves the strongest signal. When transmitting, the AP chooses the antenna with the highest success rate, and broadcasts are transmitted on alternating antennas.

Antenna diversity is enabled by default (set to “auto”) per wireless interface. When using the internal antennas, Proxim recommends leaving antenna diversity enabled. However, you may disable antenna diversity by manually selecting which antenna to use for each wireless interface through the Command Line Interface. See Configure Antenna Diversity for information.

When operating in 4.9 GHz Public Safety mode, an external 4.9 GHz antenna must be attached to the pigtail connected to Antenna connector 3 (and the corresponding internal antenna is disabled). See 4.9 GHz Antenna for information and Attaching Antenna(s) to the AP-4900M for 4.9 GHz Operation for installation instructions.

External Antennas

The AP-4000/4000M/4900M also has four antenna connectors, two on each radio, for use with external antennas. External antennas can be used with either radio on the AP-4000/4000M/4900M.

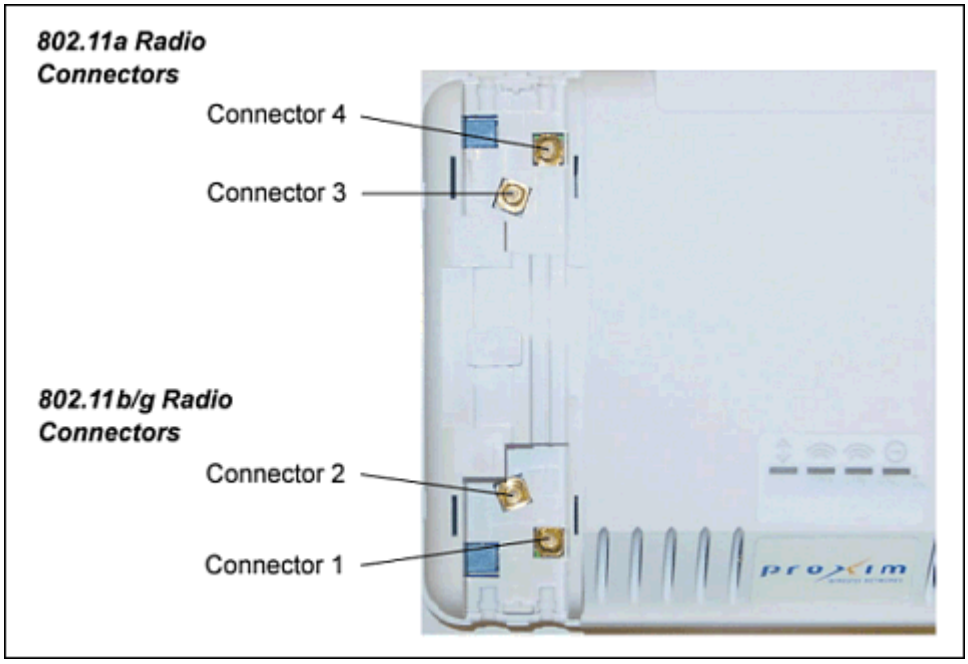


Figure 2-2 AP-4000/4000M/4900M Antenna Connectors

Connectors 1 and 2 are for the 802.11b/g radio; connectors 3 and 4 are for the 802.11a radio. When the AP is mounted on a wall, connectors 1 and 4 correspond to the horizontally polarized internal antenna, providing a coverage pattern parallel to the wall; connectors 2 and 3 correspond to the vertically polarized internal antenna, providing a coverage pattern parallel to the ceiling/floor. When the AP is mounted to a ceiling, connectors 1 and 4 correspond to the vertically polarized internal antenna, and connectors 2 and 3 correspond to the horizontally polarized internal antenna. Plugging an external antenna in to the antenna connector disables the corresponding internal antenna on the wireless interface.

The AP continues to support antenna diversity with external antennas connected. With one external antenna connected to one of the two antenna connectors on a radio, one internal antenna and one external antenna are used for antenna diversity. With two external antennas connected, both external antennas are used for antenna diversity, and both internal antennas are disabled.

With external antennas connected, you may wish to manually select a particular antenna for use. To do so, disable antenna diversity by manually selecting which antenna to use for each wireless interface through the Command Line Interface. See Configure Antenna Diversity for information.

For a list of recommended antennas, see http://www.proxim.com/products/wifi/accessories. For installation instructions, see Installing External Antennas.

4.9 GHz Antenna

On the AP-4900M, antenna connector 3 is equipped with a pigtail adaptor for connection to a 4.9 GHz antenna. When the AP-4900M is configured to operate in the 4.9 GHz Public Safety operational mode, antenna diversity is automatically disabled, and antenna 3 is statically configured for use. Connecting an external antenna to this antenna port disables the corresponding internal antenna. For a list of recommended antennas, see http://www.proxim.com/products/wifi/accessories. For installation instructions, see Attaching Antenna(s) to the AP-4900M for 4.9 GHz Operation.

Active Ethernet

The AP-4000/4000M/4900M is equipped with an 802.3af-compliant Active Ethernet module. Active Ethernet (AE) delivers both data and power to the access point over a single Ethernet cable. If you choose to use Active Ethernet, there is no difference in operation; the only difference is in the power source.

- The Active Ethernet (AE) integrated module receives ~48 VDC over a standard Category 5 Ethernet cable.
- To use Active Ethernet, you must have an AE hub (also known as a power injector) connected to the network.
- The cable length between the AE hub and the Access Point should not exceed 100 meters (approximately 325 feet). The AE hub is not a repeater and does not amplify the Ethernet data signal.
- If connected to an AE hub and an AC power simultaneously, the Access Point draws power from Active Ethernet.

Also see Hardware Specifications.

NOTE: *The AP's 802.3af-compliant Active Ethernet module is backwards compatible with all ORiNOCO Active Ethernet hubs that do not support the IEEE 802.3af standard.*

LED Indicators

The top panel of the AP-4000/4000M/4900M has the following LED indicators.

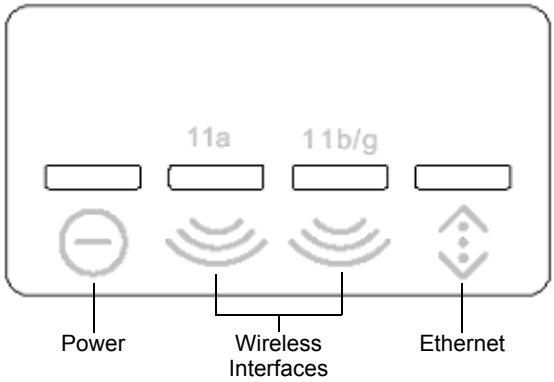


Figure 2-3 LED Indicators on the AP-4000/4000M/4900M Top Panel

The LED indicators exhibit the following behavior:

Indication	Power	Wireless Interface A (802.11a radio)	Wireless Interface B (802.11b/g radio)	Ethernet
Solid Green	AP image running.	Wireless interface A is preparing for use.	Wireless interface B is preparing for use.	Ethernet interface is connected at 100 Mbps with no traffic.
Blinking Green	n/a	Wireless interface A is transmitting or receiving wireless packets.	Wireless interface B is transmitting or receiving wireless packets.	Ethernet interface is connected at 100 Mbps with traffic.
Solid Amber	The Bootloader is loading the application software.	n/a	n/a	Ethernet interface is connected at 10 Mbps with no traffic.
Blinking Amber	The AP is reloading.	n/a	n/a	The Ethernet interface is connected at 10 Mbps with traffic.
Solid Red	Power On Self Test (POST) running.	n/a	n/a	n/a
Blinking Red	Rebooting.	n/a	n/a	n/a

Prerequisites

General Prerequisites

Before installing an AP-4000/4000M/4900M, you need to gather certain network information. The following table identifies the information you need.

Network Name (SSID of the wireless cards)	You must assign the Access Point a Network Name before wireless users can communicate with it. The clients also need the same Network Name. This is not the same as the System Name, which applies only to the Access Point. The network administrator typically provides the Network Name.
AP's IP Address	If you do not have a DHCP server on your network, then you need to assign the Access Point an IP address that is valid on your network.
HTTP Password	Each Access Point requires a read/write password to access the web interface. The default password is "public".
CLI Password	Each Access Point requires a read/write password to access the CLI interface. The default password is "public".
SNMP Read Password	Each Access Point requires a password to allow get requests from an SNMP manager. The default password is "public".
SNMP Read-Write Password	Each Access Point requires a password to allow get and set requests from an SNMP manager. The default password is "public".
SNMPv3 Authentication Password	If Secure Management is enabled, each Access Point requires a password for sending authenticated SNMPv3 messages. The default password is "public". The default SNMPv3 username is administrator, with SHA authentication, and DES privacy protocol.
SNMPv3 Privacy Password	If Secure Management is enabled, each Access Point requires a password when sending encrypted SNMPv3 data. The default password is "public".
Security Settings	You need to determine what security features you will enable on the Access Point.
Authentication Method	A primary authentication server may be configured; a backup authentication server is optional. The network administrator typically provides this information.
Authentication Server Shared Secret	This is a password shared between the Access Point and the RADIUS authentication server (so both passwords must be the same), and is typically provided by the network administrator.
Authentication Server Authentication Port	This is a port number (default is 1812) and is typically provided by the network administrator.
Client IP Address Pool Allocation Scheme	The Access Point can automatically provide IP addresses to clients as they sign on. The network administrator typically provides the IP Pool range.
DNS Server IP Address	The network administrator typically provides this IP Address.
Gateway IP Address and Subnet Mask	The gateway IP address and subnet mask of the network environment where the Access Point is deployed.

Mesh Prerequisites

Before setting up a Mesh network, gather the following information:

Mesh Mode	The mode in which the AP will be used. If the AP will be connected directly to the wired backbone, it should be configured for Mesh Portal mode; if it will connect to the Portal and backbone wirelessly, it should be configured for Mesh AP mode. If the AP will not be used in a Mesh network, Mesh Mode can be disabled.
Mesh Interface Number	The interface on which the Mesh functionality will be enabled. For Wireless A, the interface number is 3; for Wireless B, the interface number is 4.
Mesh SSID	The name of the Mesh network. The Mesh SSID should be between 1 and 16 characters.
Mesh Security Mode	Mesh links may be secured through AES encryption. You may also choose to use Mesh functionality without security enabled.
Mesh AP Shared Secret	The password shared between Mesh Access Points when AES is enabled (AES is enabled by default). This password should be between 6 and 32 characters. The default password is “public.”

Product Package

Each AP-4000/4000M/4900M comes with the following:

- AP-4000/4000M/4900M unit (with integrated 802.11a radio and 802.11b/g radio, and Active Ethernet)
- Power adapter
- One ceiling or wall mounting plate
- Security cover
- One Installation CD-ROM that contains the following:
  - Software Installation Wizard
  - ScanTool
  - MIBs
  - User's Guide in PDF format
  - Xtras folder containing the following
    - SolarWinds® TFTP software
    - Ekahau™ Site Survey software
    - Acrobat® Reader software
- One *Quick Start Flyer*

If any of these items are missing or damaged, please contact your reseller or Technical Support (see Technical Support for contact information).

System Requirements

To begin using an AP, you must have the following minimum requirements:

- A 10Base-T Ethernet or 100Base-TX Fast Ethernet switch or hub or cross-over Ethernet cable
- At least one of the following IEEE 802.11-compliant devices:
  - An 802.11a, 802.11b, or 802.11b/g client device
- A computer that is connected to the same IP network as the AP and has one of the following Web browsers installed:
  - Microsoft® Internet Explorer 6 with Service Pack 1 or later and patch Q323308
  - Netscape® 7.1 or later

  (The computer is required to configure the AP using the HTTP interface.)

Hardware Installation

NOTE:
Before installing and using this product, see the Regulatory Compliance **section.**

NOTE:
Avant l'installation et l'utilisation de ce produit, veuillez vous référer à la partie « Regulatory Compliance **» (conformité aux réglementations).**

NOTA:
Prima di installare ed utilizzare questo prodotto, fare riferimento alla sezione relativa alla "Regulatory Compliance**" (conformità alle norme).**

ANMERKUNG:
Bitte lesen Sie vor der Installation und Verwendung dieses Produkts im Abschnitt „Regulatory Compliance**".**

NOTA:
Antes de instalar y usar este producto, consulte la sección "Regulatory Compliance**" (Cumplimiento de la normativa).**

注記：
製品をインストールしてご使用になる前に、の「Regulatory Compliance」セクションを参照し、使用許諾に関する重要な事項を確認してください。

Required Materials

- AP-4000/4000M/AP-4900M unit
- Mounting bracket with screws
- Power adapter
- Security cover
- *Quick Start Flyer*

Perform the following procedures to install the AP hardware:

- Cabling the AP-4000/4000M/4900M
- Installing the Security Cover
- Mounting the AP-4000/4000M/4900M
- Installing External Antennas

Cabling the AP-4000/4000M/4900M

Connect cables to the AP as follows:

1. Provide power to the AP, as follows:
   a. Plug the power cord into the power jack (the left port) and connect the unit to an AC power outlet (100~240V, 50~60Hz).
   b. If using Active Ethernet, connect power to the unit from a DC injector device, such as the ORiNOCO 1-Port Active Ethernet DC Injector hub.

2. Attach one end of an Ethernet cable to the AP's LAN port (the center port, labeled “LAN”) and the other end to a network hub or switch.
3. Optionally, connect an RS-232 cable to the RS-232 console port (the right port, labeled “RS-232”).

NOTE: *You cannot install the security cover to the AP-4000/4000M/4900M if an RS-232 cable is connected.*

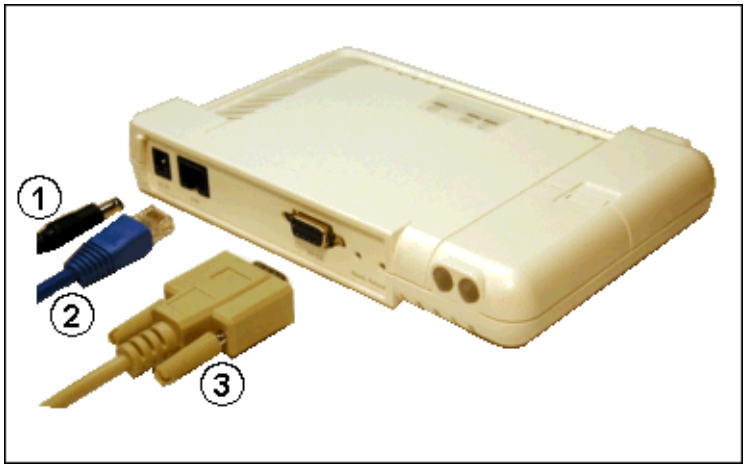


Figure 2-4 Cabling the AP-4000/4000M/4900M

4. Verify LED Status
5. When the AP-4000/4000M/4900M boots, it performs a series of self-tests.
6. Wait for the power LED to turn green before proceeding.

Installing the Security Cover

You can optionally install a security cover to deter unauthorized access to the AP-4000. The security cover is a plastic cover that prevents access to the cabling and to the Reset and Reload buttons.

NOTE: *You cannot connect an RS-232 cable to the AP-4000/4000M/4900M when a security cover is installed.*

1. Slide the hinging end of the security cover into the hole on the rear panel of the AP-4000/4000M/4900M to the left of the connectors.
2. Use two screws to screw the right side of the security cover to the RS-232 screw holes on the rear panel of the AP-4000.

Mounting the AP-4000/4000M/4900M

Proxim recommends that you have a site survey professionally conducted to determine the best location for the AP. For professional site surveyors, Ekahau Site Survey software is included in the Xtras folder on the Installation CD-ROM.

The following considerations must be kept in mind when the AP-4900M is mounted in a vehicle or outdoors:

- The AP must be protected from exposure, and the environmental conditions must be within those specified in the product datasheet that can be found at http://www.proxim.com/products/wifi/ap/. To most easily comply with these specifications, Proxim recommends mounting the AP-4900M in the passenger compartment of a vehicle or in a weatherproof NEMA box outdoors.
- When the AP is mounted within a vehicle, the metallic skin of the vehicle will retard the RF propagation of the AP.
- Proxim recommends the 1086-PGTL adapter with an external vehicular antenna. For more information,, see http://www.proxim.com/products/wifi/accessories.
- The AP-4900M uses 5 V, not 12 V power. Therefore a 12V-to-5V transformer will be needed when mounting the AP in a vehicle.

Once you have chosen a final location for your unit, mount the AP-4000/4000M/4900M to a wall, to a T-bar ceiling, or in a vehicle as described below.

Mounting the AP-4000/4000M/4900M to a Ceiling

1. Attach the mounting plate to the bottom of the AP-4000/4000M/4900M by lining up the keyholes and attaching it with two screws.
2. Snap the tabs onto the ceiling T-bar. Rotate the AP-4000/4000M/4900M until it snaps on to the T-bar.

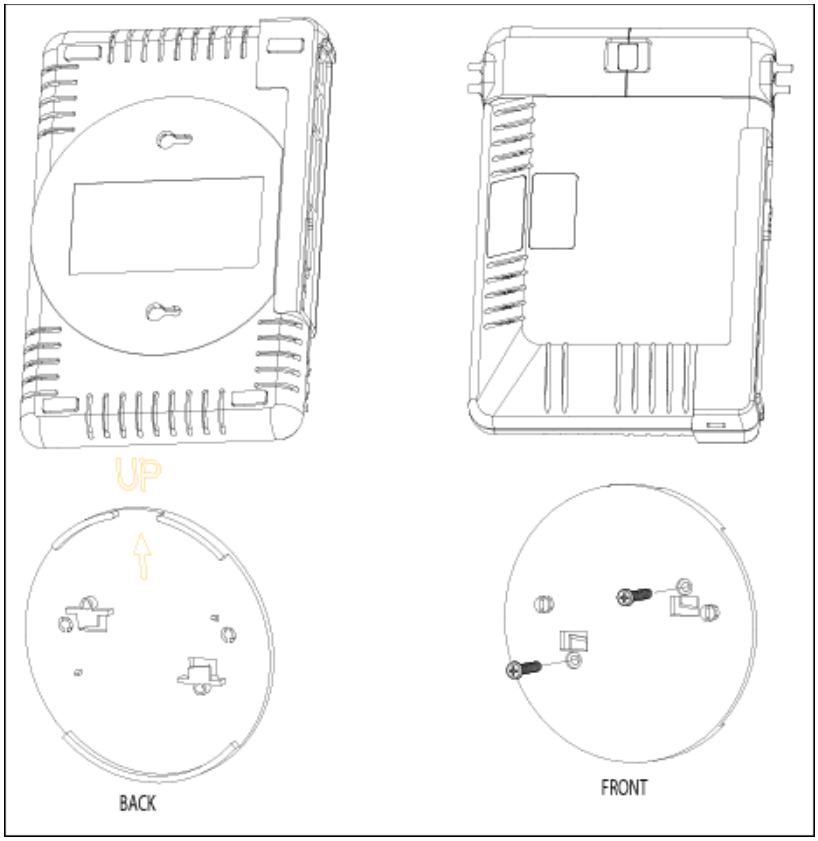


Figure 2-5 AP-4000/4000M/4900M Mounting Plate

Mounting the AP-4000/4000M/4900M to a Wall

1. Put the mounting plate up to the wall.
2. Screw through the mounting plate.
3. Place the AP up against the mounting plate. Orient the AP with the long access vertical, with the connectors facing to the left.

Mounting the AP-4900M in a Vehicle

1. Attach the mounting plate up to the wall or to the wall partition (cage) behind the passenger seat in a vehicle. The knobs that fit into the keyholes on the AP-4900M should be in a vertical line.
2. Screw through the mounting plate.
3. Place the AP up against the mounting plate. Orient the AP with the long access vertical, with the connectors facing right.

Installing External Antennas

You can optionally install external antennas on the AP-4000/4000M/4900M. For information on the AP's antenna functionality, see Antennas.

Follow the mounting instructions included with your external antenna, and then connect the antenna cable to the AP, as follows:

1. Press down near the center of the compartment covering and slide open the external antenna access compartments. The compartment closer to the LED panel contains the connectors for the 802.11b/g radio, and the other compartment contains the connectors for the 802.11a radio.

   NOTE: *AP-4000 models 8670-US2 and 8670-AU do not provide external antenna connectors for 5GHz (802.11a) operation.*

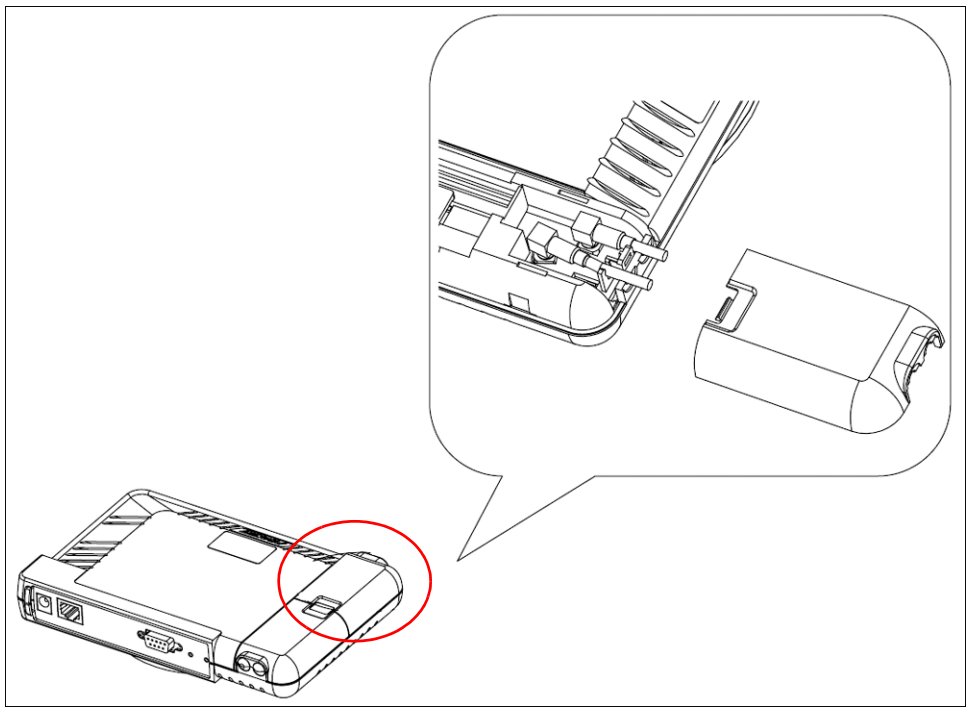


Figure 2-6 Opening the Antenna Compartment

2. There are four antenna connectors in the AP-4000/4000M/4900M, labeled 1 through 4. Connectors 1 and 2 are for the 802.11b/g radio, and connectors 3 and 4 and for the 802.11a radio.Connect the antenna cable to connector 1 or 4 (the connector closer to the LED panel in the compartment), depending on the radio.

   NOTE: *When the AP-4900M is configured to operate in the 4.9 GHz Public Safety operational mode, antenna diversity is disabled, and antenna 3 is statically configured for use.*

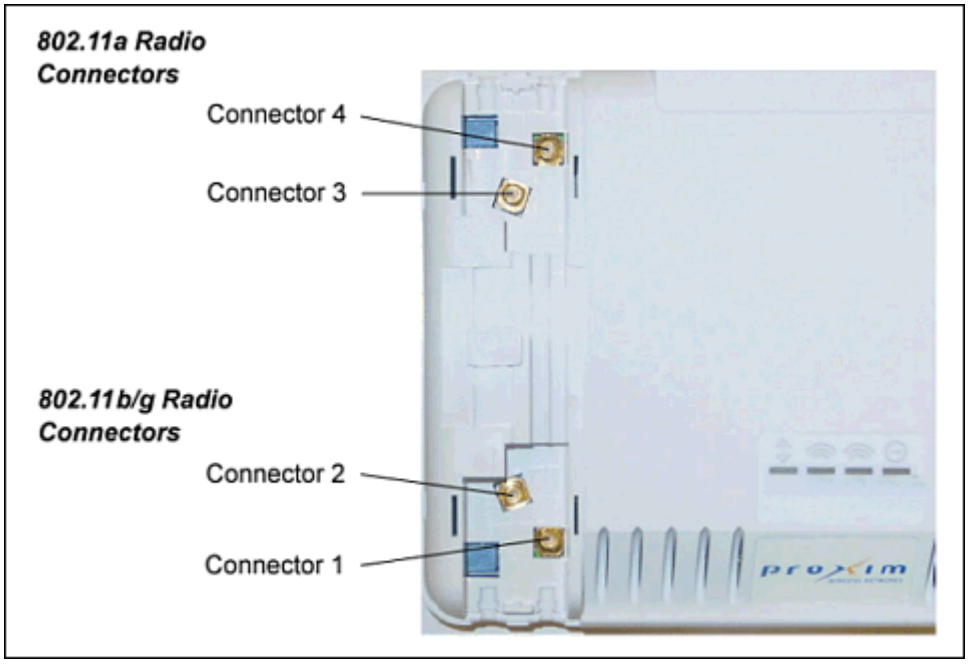


Figure 2-7 AP-4000/4000M/4900M Antenna Connectors

3. If installing a second external antenna on a radio, connect the antenna cable to connector 2 (802.11b/g radio) or connector 3 (802.11a radio).
4. Close the external antenna access compartments.
5. If desired, manually select which antenna(s) to use through the Command Line Interface. See Configure Antenna Diversity.

Attaching Antenna(s) to the AP-4900M for 4.9 GHz Operation

To attach an external antenna to the AP-4900M, attach the selected antenna to the pigtail attachment connected to the AP's antenna connector 3 (see Figure 2-8).

For a list of recommended antennas, see http://www.proxim.com/products/wifi/accessories.

Figure 2-8 AP-4900M External Antenna Connection

Installing the AP in a Plenum

In an office building, plenum is the space between the structural ceiling and the tile ceiling that is provided to help air circulate. Many companies also use the plenum to house communication equipment and cables. These products and

cables must comply with certain safety requirements, such as Underwriter Labs (UL) Standard 2043: “Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces”.

The AP-4000/4000M/4900M has been certified under UL Standard 2043 and can be installed in the plenum.

When installed in a plenum, the AP must use Active Ethernet.

Initialization

The following sections detail how to initialize the AP using ScanTool, log in to the HTTP interface, perform an initial configuration of the AP using the Setup Wizard, and download the required AP software.

- Using ScanTool
- Logging In
- Using the Setup Wizard
- Installing the Software

Using ScanTool

ScanTool is a software utility that is included on the installation CD-ROM. It is an initial configuration tool that allows you to find the IP address of an Access Point by referencing the MAC address in a Scan List, or to assign an IP address if one has not been assigned.

The tool automatically detects the Access Points installed on your network, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use set initial device parameters that will allow the AP to retrieve a new software to an AP that does not have a valid software image installed (see Client Connection Problems).

To access the HTTP interface and configure the AP, the AP must be assigned an IP address that is valid on its Ethernet network. By default, the AP is configured to obtain an IP address automatically from a network Dynamic Host Configuration Protocol (DHCP) server during boot-up. If your network contains a DHCP server, you can run ScanTool to find out what IP address the AP has been assigned. If your network does not contain a DHCP server, the Access Point's IP address defaults to 169.254.128.132. In this case, you can use ScanTool to assign the AP a static IP address that is valid on your network.

NOTE: *Mesh APs must have static IP addresses, as the DHCP client will not function on wireless interfaces.*

ScanTool Instructions

Follow these steps to install ScanTool and initialize the AP:

1. Locate the unit's Ethernet MAC address and write it down for future reference. The MAC address is printed on the product label. Each unit has a unique MAC address, which is assigned at the factory.
2. Confirm that the AP is connected to the same LAN subnet as the computer that you will use to configure the AP.
3. Power up, reboot, or reset the AP.

   The unit requests an IP Address from the network DHCP server.
4. Insert the Installation CD into the CD-ROM drive of the computer that you will use to configure the AP.

   The installation program will launch automatically.
5. Follow the on-screen instructions to install the Access Point software and documentation.

   NOTE: *The ORiNOCO Installation program supports the following operating systems:*

   - Windows® 98SE
   - Windows® 2000
   - Windows® NT
   - Windows® ME
   - Windows® XP
6. After the software has been installed, double-click the **ScanTool** icon on the Windows desktop to launch the program (if the program is not already running).

   ScanTool scans the subnet and displays all detected Access Points. The ScanTool's ***Scan List*** screen appears, as shown in the following example.

NOTE: *If your computer has more than one network adapter installed, you will be prompted to select the adapter that you want ScanTool to use before the* ***Scan List*** *appears. If prompted, select an adapter and click* **OK**. *You can change your adapter setting at any time by clicking the* **Select Adapter** *button on the* ***Scan List*** *screen. Note that the* ***ScanTool Network Adapter Selection*** *screen will not appear if your computer only has one network adapter installed.*

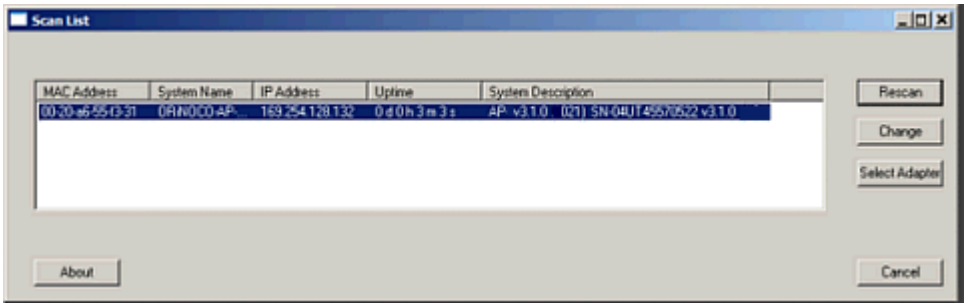


Figure 2-9 Scan List

7. Locate the MAC address of the AP you want to initialize within the Scan List.

   NOTE: *If your Access Point does not show up in the Scan List, click the* **Rescan** *button to update the display. If the unit still does not appear in the list, see* Troubleshooting *for suggestions. Note that after rebooting an Access Point, it may take up to five minutes for the unit to appear in the Scan List.*

8. Do one of the following:
   - If the AP has been assigned an IP address by a DHCP server on the network, write down the IP address and click **Cancel** to close ScanTool. Proceed to the Logging In section for information on how to access the HTTP interface using this IP address.

     NOTE: *Mesh APs must be configured with static IP addresses. To assign the AP a static IP address, follow the steps below.*

   - If the AP has not been assigned an IP address (in other words, the unit is using its default IP address, 169.254.128.132), follow these steps to assign it a static IP address that is valid on your network:
     a. Highlight the entry for the AP you want to configure.
     b. Click the **Change** button.

        The ***Change*** screen appears.

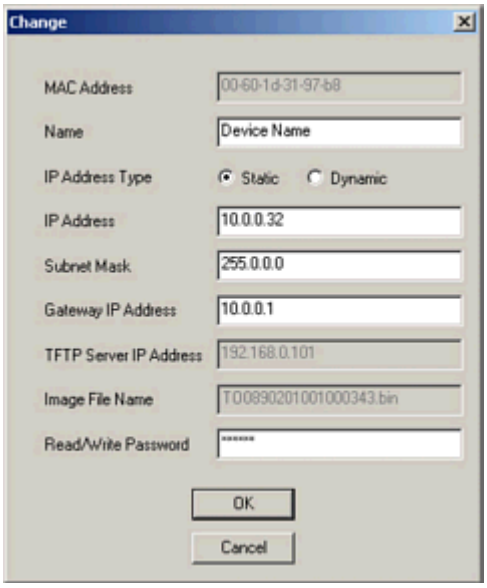


Figure 2-10 Scan Tool Change Screen

c. Set **IP Address Type** to **Static**.

d. Enter a static **IP Address** for the AP in the field provided. You must assign the unit a unique address that is valid on your IP subnet. Contact your network administrator if you need assistance selecting an IP address for the unit.

e. Enter your network's **Subnet Mask** in the field provided.

f. Enter your network's **Gateway IP Address** in the field provided.

g. Enter the SNMP Read/Write password in the **Read/Write Password** field (for new units, the default SNMP Read/Write password is "public").

NOTE: *The TFTP Server IP Address and Image File Name fields are only available if ScanTool detects that the AP does not have a valid software image installed. See* Client Connection Problems*.*

h. Click **OK** to save your changes.

i. The Access Point will reboot automatically and any changes you made will take effect.

j. When prompted, click **OK** a second time to return to the ***Scan List*** screen.

k. Click **Cancel** to close the ScanTool.

Logging In

Once the AP has a valid IP Address and an Ethernet connection, you may use your web browser to monitor and configure the AP. (To configure and monitor using the command line interface, see Command Line Interface (CLI).)

1. Open a Web browser on a network computer.
   – The HTTP interface supports the following Web browsers:
      • Microsoft® Internet Explorer 6 with Service Pack 1 or later
      • Netscape® 7.1 or later
2. If necessary, disable the browser's Internet proxy settings. For Internet Explorer users, follow these steps:
   – Select **Tools > Internet Options**.
   – Click the **Connections** tab.
   – Click **LAN Settings**.
   – If necessary, remove the check mark from the **Use a proxy server** box.

– Click **OK** twice to save your changes and return to Internet Explorer.

3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter** or **Go**.

   This is either the dynamic IP address assigned by a network DHCP server or the static IP address you manually configured. See Using ScanTool for information on how to determine the unit's IP address and manually configure a new IP address, if necessary.

   NOTE: *Mesh APs must be configured with static IP addresses.*

   The ***Enter Network Password*** screen appears.

Figure 2-11 Enter Network Password

4. Enter the HTTP password in the **Password** field. Leave the **User Name** field blank. For new units, the default HTTP password is **public**.

   If you are logging on for the first time the **Setup Wizard** will launch automatically.

   NOTE: *To prevent the Setup Wizard from launching upon log in, click on* ***Management*** > ***Services*** *and choose* ***Disable*** *from the* ***Setup Wizard*** *drop down menu.*

5. Follow the steps below to configure the AP using the Setup Wizard (see Using the Setup Wizard), or click **Exit** to configure the system manually. Upon clicking **Exit**, the **System Status** screen will appear.

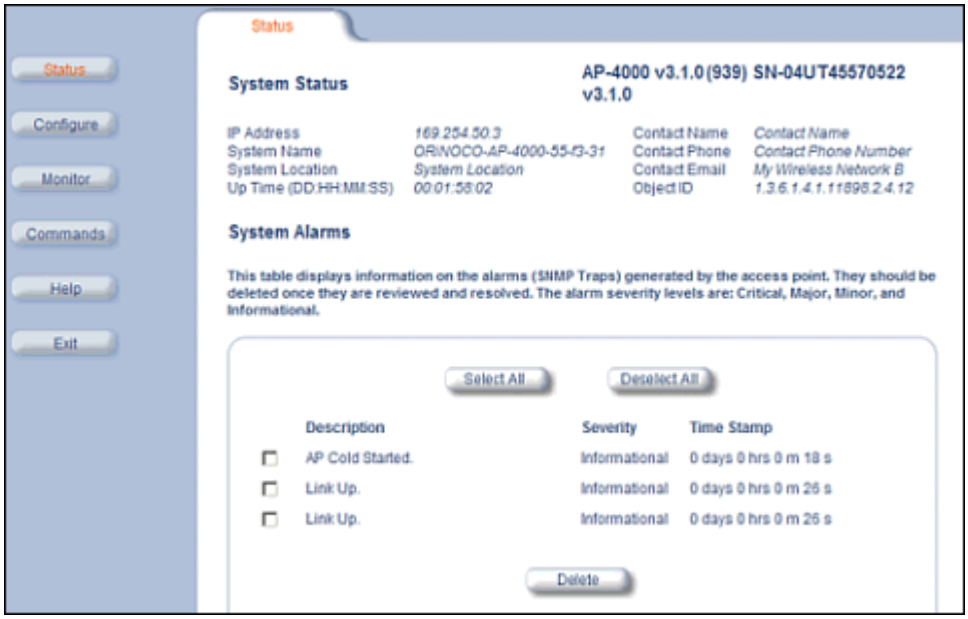


Figure 2-12 System Status Screen

The buttons on the left of the screen provide access to the monitoring and configuration options for the AP. See Advanced Configuration to begin configuring the AP without using the Setup Wizard.

The Command Line Interface (CLI) also provides a method for monitoring and configuring the AP using Telnet or a serial connection. For more information about monitoring and configuring the AP with the CLI, see Command Line Interface (CLI).

Using the Setup Wizard

The first time you connect to an AP's HTTP interface, the Setup Wizard launches automatically. The Setup Wizard provides step-by-step instructions for how to configure the Access Point's basic operating parameters, such as Network Name, IP parameters, system parameters, and management passwords.

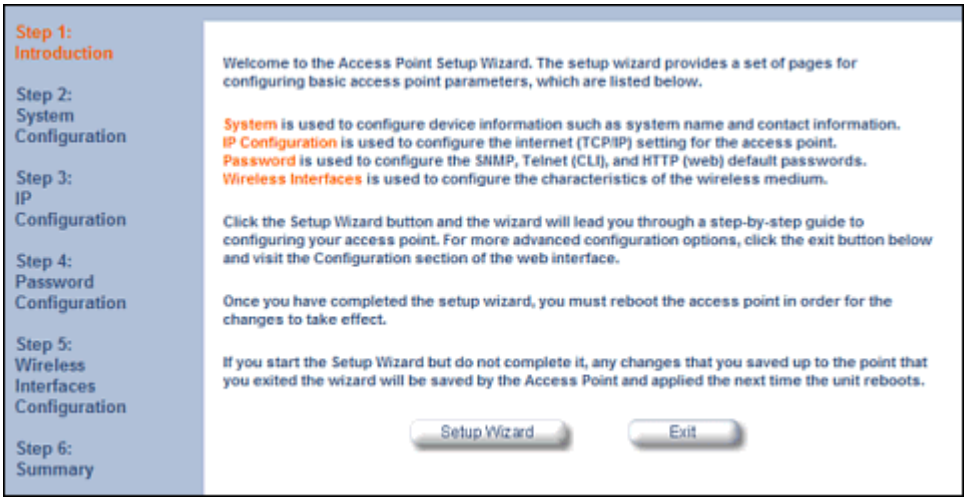


Figure 2-13 Setup Wizard

Setup Wizard Instructions

1. Click **Setup Wizard** to begin. The Setup Wizard supports the following navigation options:
   - **Save & Next Button:** Each Setup Wizard screen has a **Save & Next** button. Click this button to submit any changes you made to the unit's parameters and continue to the next page. The instructions below describe how to navigate the Setup Wizard using the **Save & Next** buttons.
   - **Navigation Panel:** The Setup Wizard provides a navigation panel on the left-hand side of the screen. Click the link that corresponds to the parameters you want to configure to be taken to that particular configuration screen. Note that clicking a link in the navigation panel will not submit any changes you made to the unit's configuration on the current page.
   - **Exit:** The navigation panel also includes an **Exit** option. Click this link to close the Setup Wizard at any time.

     CAUTION: *If you exit from the Setup Wizard, any changes you submitted (by clicking the **Save & Next** button) up to that point will be saved to the unit but will not take effect until it is rebooted.*
2. Configure the System Configuration settings and click **Save & Next**. See System for more information.
3. Configure the Access Point's Basic IP address settings, if necessary, and click **Save & Next**. See Basic IP Parameters for more information.
4. Assign the AP new passwords to prevent unauthorized access and click **Save & Next**. Each management interface has its own password:
   - SNMP Read Password
   - SNMP Read-Write Password
   - CLI Password
   - HTTP (Web) Password

   By default, each of these passwords is set to "public". See Passwords for more information.
5. Configure the basic **Wireless Interface Configuration** settings:
   - Select the Operational Mode as follows and click **Save & Next**:

     The Wireless-A interface operates only in 802.11a mode on the AP-4000/4000M and in either 802.11a mode or 4.9 GHz Public Safety mode on the AP-4900M. The Wireless-B interface can be configured to operate in the following modes:
     - 802.11b mode only: The radio uses the 802.11b standard only.
     - 802.11g mode only: The radio is optimized to communicate with 802.11g devices. This setting will provide the best results if this radio interface will only communicate with 802.11g devices.
     - 802.11b/g mode: This is the default mode. Use this mode if you want to support a mix of 802.11b and 802.11g devices.
     - 802.11g-wifi: 802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

     In general, you should use either 802.11g only mode (if you want to support 802.11g devices only) or 802.11b/g mode to support a mix of 802.11b and 802.11g devices.
   - Configure the following available options and click **Save & Next:**
     - **Primary Network Name (SSID):** Enter a Network Name (between 1 and 32 characters long) for the wireless network. You must configure each wireless client to use this name as well. Note that the AP-4000/4000M/4900M supports up to 16 SSIDs and VLANs per wireless interface (radio). Please see the Advanced Configuration chapter for information on the detailed rules on configuring multiple SSIDs, VLANs, and security profiles.

       NOTE: *Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.*

- **Auto Channel Select:** By default, the AP scans the area for other Access Points and selects the best available communication channel, either a free channel (if available) or the channel with the least amount of interference. Remove the check mark to disable this option. See Dynamic Frequency Selection/Radar Detection (DFS/RD) for information and Available Channels for a list of available channels.

  NOTE: *When an AP is configured to function as a Mesh AP, its channel will depend on the channel of its neighbors.*

- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See Dynamic Frequency Selection/Radar Detection (DFS/RD) for details more information and Available Channels for a list of available channels.

  NOTE: *When an AP is configured to function as a Mesh AP, its channel will depend on the channel of its neighbors.*

- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP-4000/4000M/4900M's radios. The Auto Fallback feature allows the AP to select the best transmit rate based on the cell size.
  - For the 802.11a radio operating in 802.11a mode, choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback.
  - For the 802.11a radio operating in 4.9 GHz Public Safety mode, choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback.
  - These transmit rates are based on a 20 MHz channel bandwidth (the default). Additional rates are available with 10 MHz channel bandwidths. To select alternate bandwidths and transmit rates, see Operational Mode.
  - For the 802.11b/g radio operating in 802.11b mode, choose between 1, 2, 5.5, 11 Mbits/s, and Auto Fallback.
  - For the 802.11b/g radio operating in 802.11g mode, choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback.
  - For the 802.11b/g radio operating in 802.11b/g mode, choose between 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec, and Auto Fallback.
  - For the 802.11b/g radio operating in 802.11g-wifi mode, choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback.

    NOTE: *802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.*

Additional advanced settings are available in the ***Wireless Interface Configuration*** screen. See Interfaces for details. See Security Profile for a description of security features, Management VLAN for a description of VLAN capabilities, and Configuring Security Profiles for detailed configuration procedures.

6. Review the configuration summary. If you want to make any additional changes, use the navigation panel on the left-hand side of the screen to return to an earlier screen. After making a change, click **Save & Next** to save the change and proceed to the next screen.
7. When finished, click **Reboot** on the Summary screen to restart the AP and apply your changes.

Installing the Software

Proxim periodically releases updated software for the AP on its Web site, http://support.proxim.com (Knowledgebase Answer ID 1250). Proxim recommends that you check the Web site for the latest updates after you have installed and initialized the unit.

Download the Software

1. In your web browser, go to http://support.proxim.com.

2. If prompted, create an account to gain access.

   NOTE: *The Knowledgebase is available to all website visitors. First-time users will be asked to create an account to gain access.*

3. Click **Search Knowledgebase**.
4. In the **Search Knowledgebase** field, enter **1250**.
5. From the **Search By** drop-down menu, select Answer ID.
6. Click **Search**.
7. Click on the appropriate link to download the software.
8. Use the instructions in the following sections to install the new software.

Install Software with HTTP Interface

Use the **Update AP via HTTP** tab to update the AP with the latest software image.

1. Click **Commands** > **Update AP** > **via HTTP**.

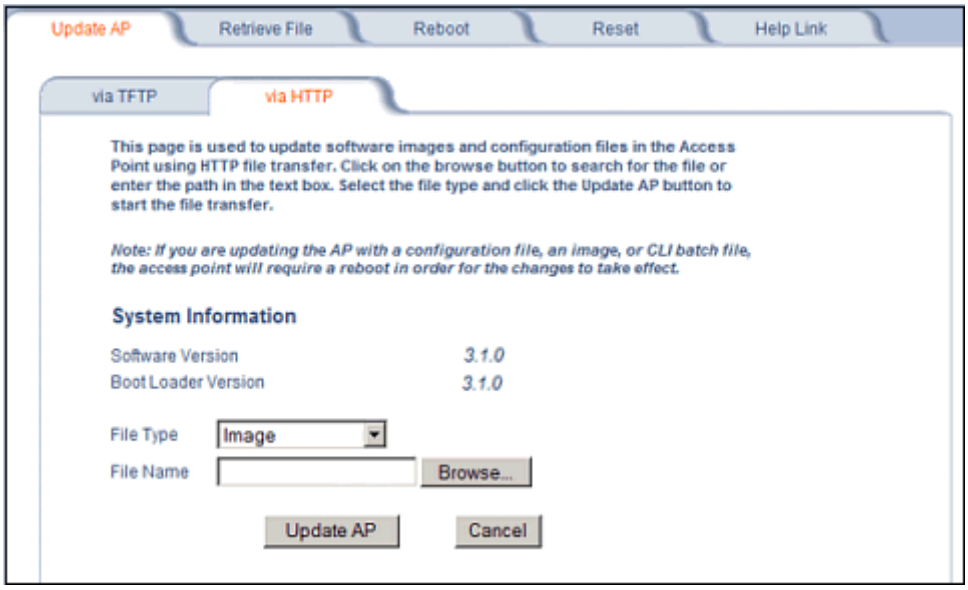


Figure 2-14 Update AP via HTTP Command Screen

2. From the File Type drop-down menu, select **Image**.
3. Use the **Browse** button to locate or manually type in the name of the file (including the file extension) the file you downloaded from the Proxim Knowledgebase. If typing the file name, you must include the full path and the file extension in the file name text box.
4. To initiate the HTTP Update operation, click the **Update AP** button.

   A warning message is displayed that advises the user that a reboot of the device will be required for changes to take effect.

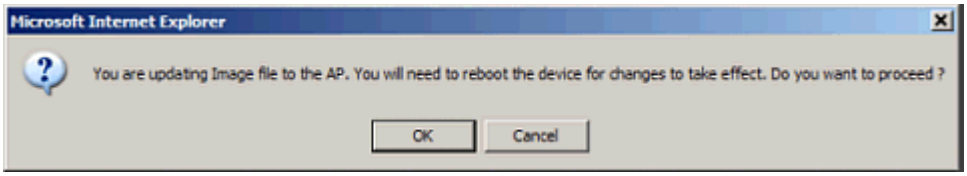


Figure 2-15 Warning Message

5. Click **OK** to continue with the operation or **Cancel** to abort the operation.
6. If the operation is unsuccessful, you will receive an error message. If this occurs, see the Troubleshooting chapter or attempt installing the software with a TFTP server, as described in the next section.
7. If the operation is successful, you will receive a confirmation message. For installation changes to take effect, reboot the AP as follows:
   - Click **Commands** > **Reboot**.
   - Enter **0** in the **Time to Reboot f**ield.
   - Click **OK**.

Install Software with TFTP Server

A Trivial File Transfer Protocol (TFTP) server allows you to transfer files across a network. You can upload files from the AP for backup or copying, and you can download the files for configuration and AP Image upgrades. The Solarwinds TFTP server software is located on the ORiNOCO AP Installation CD-ROM. You can also download the latest TFTP software from Solarwind's Web site at http://www.solarwinds.net.

NOTE: *If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface.See* Update AP via HTTP*.*

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP address, the proper AP Image file name, and that the TFTP server is operational.
- Make sure the TFTP server is configured to both Transmit and Receive files, with no automatic shutdown or time-out.

The following types of files can be downloaded to the AP from a TFTP server:

- Config (configuration file)
- Image (AP software image or kernel)
- UpgradeBspBl (BSP/Bootloader firmware file)
- License file
- SSL Certificate
- SSL Private Key
- SSH Public Key
- SSH Private Key
- CLI Batch File

Install Updates from your TFTP Server using the Web Interface

1. Download the latest software from http://support.proxim.com (Knowledgebase Answer ID 1250). See Download the Software for instructions).
2. Copy the latest software updates to your TFTP server.
3. In the Web Interface, click the **Commands** button and select the **Download** tab.
4. Enter the **IP address** of your TFTP server in the field provided.
5. Enter the **File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
6. Select the **File Type** from the drop-down menu (use *Img* for software updates).
7. Select **Download & Reboot** from the **File Operation** drop-down menu.
8. Click **OK**. The Access Point will reboot automatically when the download is complete.

Install Updates from your TFTP Server using the CLI

1. Download the latest software to http://support.proxim.com (Knowledgebase Answer ID 1250). See Download the Software for instructions).
1. Copy the latest software updates to your TFTP server.
2. Open the CLI interface via Telnet or a serial connection.
3. Enter the CLI password when prompted.
4. Enter the command: **`download <tftpaddr> <filename> img`**

   The download will begin, and the image will be downloaded to the Access Point.
5. When the download is complete, type **`reboot 0`** and press **Enter**.

NOTE: *See* Command Line Interface (CLI) *for more information.*

Related Topics

The Setup Wizard helps you configure the basic AP settings required to get the unit up and running. The AP supports many other configuration and management options. The remainder of this user guide describes these options in detail.

- See Advanced Configuration for information on configuration options that are available within the Access Point's HTTP interface.
- See Monitoring for information on the statistics displayed within the Access Point's HTTP interface.
- See Commands for information on the commands supported by the Access Point's HTTP interface.
- See Troubleshooting for troubleshooting suggestions.
- See Command Line Interface (CLI) for information on the CLI interface and for a list of CLI commands.

3 System Status

The first screen displayed after Logging In is the ***System Status*** screen. You can always return to this screen by clicking the **Status** button.

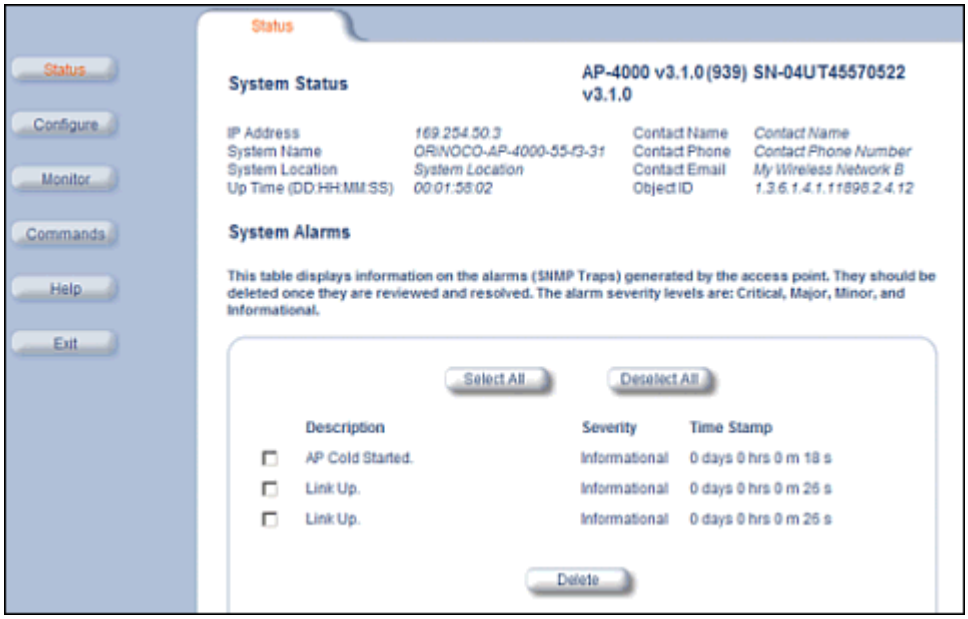


Figure 3-1 System Status Screen

The ***System Status*** screen provides the following information:

- **System Status:** This area provides system-level information, including the unit's IP address and contact information. See System for information on these settings.
- **System Alarms:** System traps (if any) appear in this area. Each trap identifies a specific severity level: critical, major, minor, and informational. See Alarms for a list of possible alarms.

From this screen, you can also access the AP's monitoring and configuration options by clicking on the buttons on the left of the screen.

4 Advanced Configuration

This chapter contains information on configuring settings in the following categories:

- System: Configure specific system information such as system name and contact information.
- Network: Configure IP, DNS client, DHCP server, DHCP Relay Agent, DHCP Relay Servers, Link Integrity, and SNTP settings.
- Interfaces: Configure the Access Point's interfaces: Wireless A, Wireless B, Ethernet, and Mesh settings. Configure the Channel Blacklist Table and a Wireless Distribution System (WDS).
- Management: Configure the Access Point's management Passwords, IP Access Table, and Services such as configuring secure or restricted access to the AP via SNMPv3, HTTPS, or CLI. Configure Secure Management, SSL, Secure Shell (SSH), and RADIUS Based Access Management. Set up Automatic Configuration for Static IP.
- Filtering: Configure Ethernet Protocol filters, Static MAC Address filters, Advanced filters, and Port filters.
- Alarms: Configure the Alarm (SNMP Trap) Groups, the Alarm Host Table, and the Syslog features.
- Bridge: Configure the Spanning Tree Protocol, Storm Threshold protection, Intra BSS traffic, and Packet Forwarding.
- QoS: Configure Wireless Multimedia Enhancements/Quality of Service parameters and QoS policies.
- Radius Profiles: Configure RADIUS features such as RADIUS Access Control and Accounting.
- SSID/VLAN/Security: Configure SSIDs, VLANs, and security profiles for each interface. Configure security features such as MAC Access Control, WPA, WEP Encryption, and 802.1x.

To configure the AP using the HTTP/HTTPS interface, you must first log in to a web browser. See Logging In for instructions.

You may also configure the AP using the command line interface. See Command Line Interface (CLI) for more information.

To configure the AP via HTTP/HTTPS:

1. Click the **Configure** button located on the left-hand side of the screen.

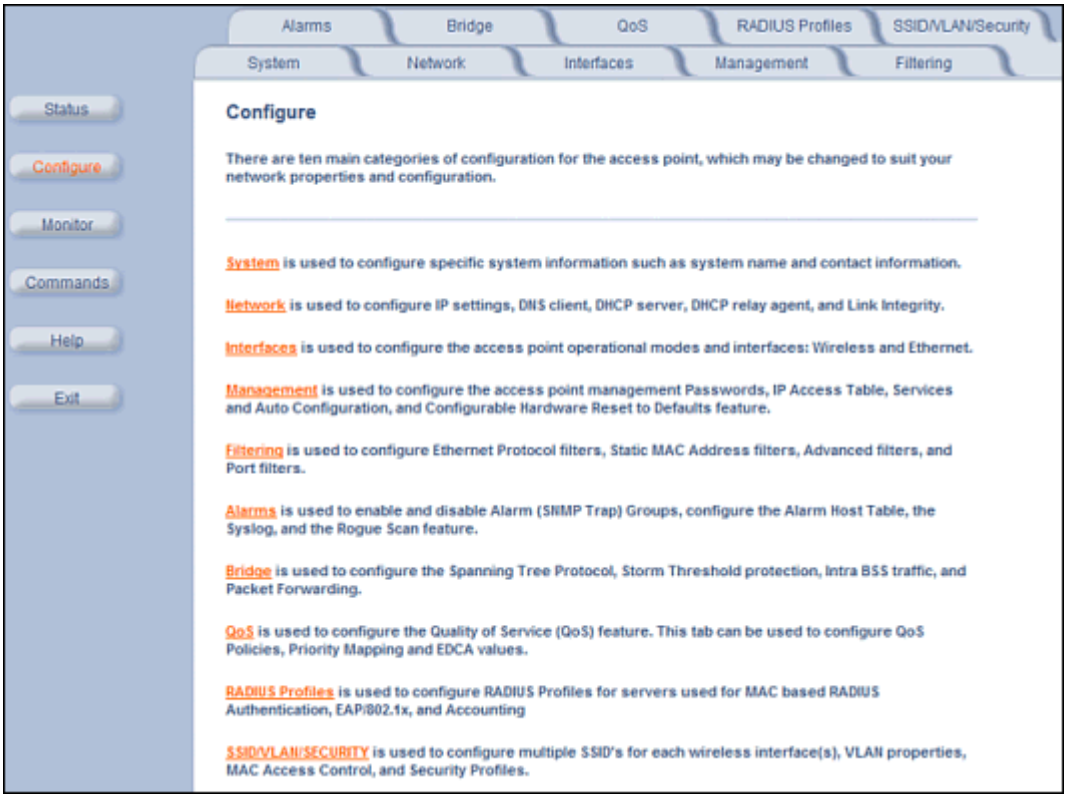


Figure 4-1 Configure Main Screen

2. Click the tab that corresponds to the parameter you want to configure. For example, click **Network** to configure the Access Point's TCP/IP settings.

Each **Configure** tab is described in the remainder of this chapter.

System

You can configure and view the following parameters within the ***System Configuration*** screen:

- **Name:** The name assigned to the AP. See the Dynamic DNS Support and Access Point System Naming Convention sections for rules on naming the AP.
- **Location:** The location where the AP is installed.
- **Contact Name:** The name of the person responsible for the AP.
- **Contact Email:** The email address of the person responsible for the AP.
- **Contact Phone:** The telephone number of the person responsible for the AP.
- **Object ID:** This is a read-only field that displays the Access Point's system object identification number; this information is useful if you are managing the AP using SNMP.
- **Ethernet MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's Ethernet interface. The MAC address is assigned at the factory.
- **Descriptor:** This is a read-only field that reports the Access Point's name, serial number, current image software version, and current bootloader software version.
- **Up Time:** This is a read-only field that displays how long the Access Point has been running since its last reboot.

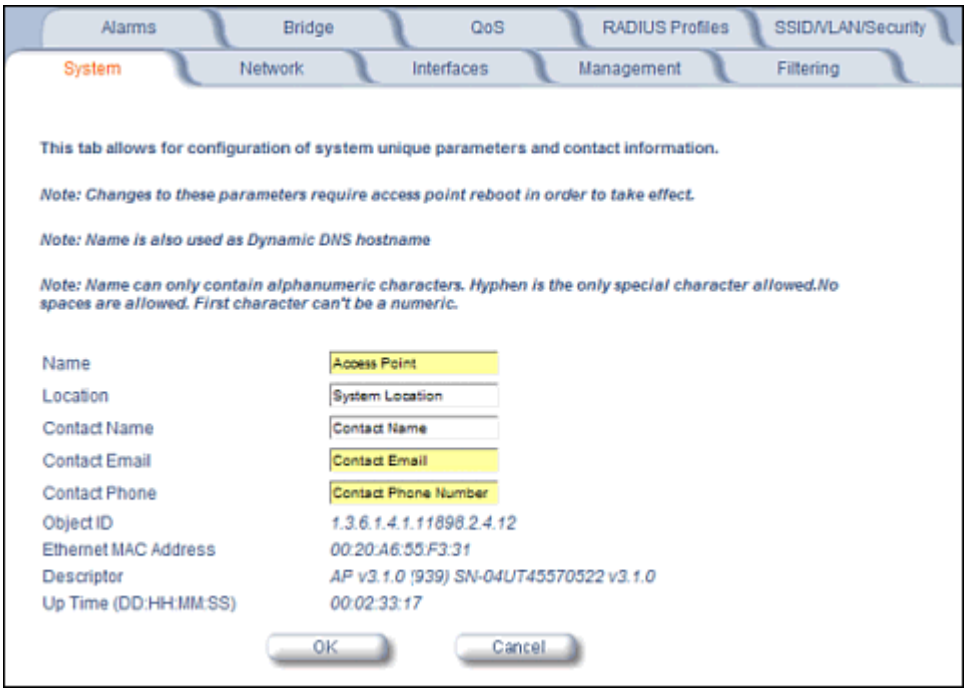


Figure 4-2 System Tab

Dynamic DNS Support

DNS is a distributed database mapping the user readable names and IP addresses (and more) of every registered system on the Internet. Dynamic DNS is a lightweight mechanism which allows for modification of the DNS data of host systems whose IP addresses change dynamically. Dynamic DNS is usually used in conjunction with DHCP for assigning meaningful names to host systems whose IP addresses change dynamically.

Access Points provide DDNS support by adding the host name (option 12) in DHCP Client messages, which is used by the DHCP server to dynamically update the DNS server.

Access Point System Naming Convention

The Access Point's system name is used as its host name. In order to prevent Access Points with default configurations from registering similar host names in DNS, the default system name of the Access Point is uniquely generated. Access Points generate unique system names by appending the last 3 bytes of the Access Point's MAC address to the default system name.

The system name must be compliant with the encoding rules for host name as per DNS RFC 1123. The DNS host name encoding rules are:

- Alphanumeric or hyphen characters are allowed.
- The name cannot start or end with a hyphen.
- The name cannot start with a digit.
- The number of characters has to be 63 or less. (Currently the system name length is limited to 32 bytes).

Network

The Network tab contains the following sub-tabs:

- IP Configuration
- DHCP Server
- DHCP Relay Agent
- Link Integrity
- SNTP (Simple Network Time Protocol)

IP Configuration

This tab is used to configure the internet (TCP/IP) settings for the access point.

These settings can be either entered manually (static IP address, subnet mask, and gateway IP address) or obtained automatically (dynamic).The DNS Client functionality can also be configured, so that host names used for configuring the access point can be resolved to their IP addresses.

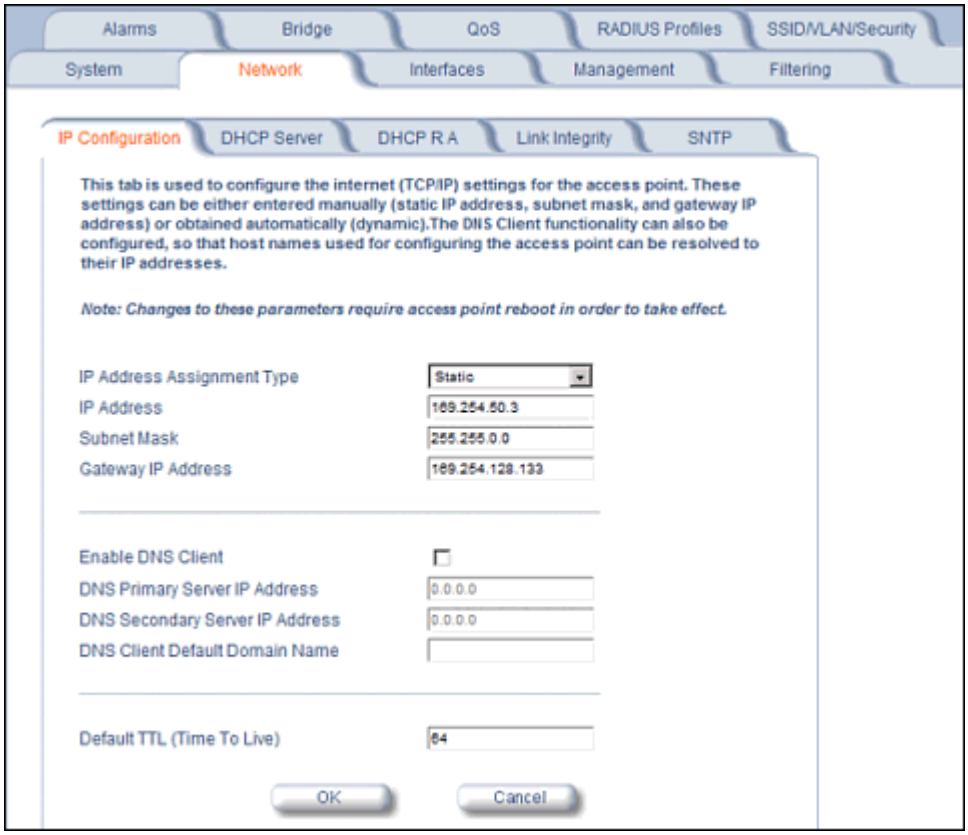


Figure 4-3 IP Configuration Sub-tab

You can configure and view the following parameters within the ***IP Configuration*** sub-tab:

NOTE: *You must reboot the Access Point in order for any changes to the Basic IP or DNS Client parameters to take effect.*

Basic IP Parameters

- **IP Address Assignment Type:** Set this parameter to **Dynamic** to configure the Access Point as a Dynamic Host Configuration Protocol (DHCP) client; the Access Point will obtain IP settings from a network DHCP server automatically during boot-up. If you do not have a DHCP server or if you want to manually configure the Access Point's IP settings, set this parameter to **Static**.

  NOTE: *IP Address Assignment Type must be set to Static if the AP will be configured as a Mesh AP.*

- **IP Address:** The Access Point's IP address. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current IP address. The Access Point will default to 169.254.128.132 if it cannot obtain an address from a DHCP server.
- **Subnet Mask:** The Access Point's subnet mask. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current subnet mask. The subnet mask will default to 255.255.0.0 if the unit cannot obtain one from a DHCP server.
- **Gateway IP Address:** The IP address of the Access Point's gateway. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the IP address of the unit's gateway. The gateway IP address will default to 169.254.128.133 if the unit cannot obtain an address from a DHCP server.

DNS Client

If you prefer to use host names to identify network servers rather than IP addresses, you can configure the AP to act as a Domain Name Service (DNS) client. When this feature is enabled, the Access Point contacts the network's DNS server to translate a host name to the appropriate network IP address. You can use this DNS Client functionality to identify RADIUS servers by host name.

- **Enable DNS Client:** Place a check mark in the box provided to enable DNS client functionality. Note that this option must be enabled before you can configure the other DNS Client parameters.
- **DNS Primary Server IP Address:** The IP address of the network's primary DNS server.
- **DNS Secondary Server IP Address:** The IP address of a second DNS server on the network. The Access Point will attempt to contact the secondary server if the primary server is unavailable.
- **DNS Client Default Domain Name:** The default domain name for the Access Point's network (for example, "proxim.com"). Contact your network administrator if you need assistance setting this parameter.

Advanced

- **Default TTL (Time to Live):** Time to Live (TTL) is a field in an IP packet that specifies the number of hops, or servers in different locations, that the request can travel before returning a failed attempt message. The Access Point uses the default TTL for generated packets for which the transport layer protocol does not specify a TTL value. This parameter supports a range from 0 to 255. By default, TTL is 64.

DHCP Server

If your network does not have a DHCP Server, you can configure the AP as a DHCP server to assign dynamic IP addresses to Ethernet nodes and wireless clients.

NOTE: *DHCP client functionality is not supported in a Mesh network.*

CAUTION: *Make sure there are no other DHCP servers on the network and do not enable the DHCP server without checking with your network administrator first, as it could disrupt normal network operation. Also, the AP must be configured with a static IP address before enabling this feature.*

When the DHCP Server functionality is enabled, you can create one or more IP address pools from which to assign addresses to network devices.

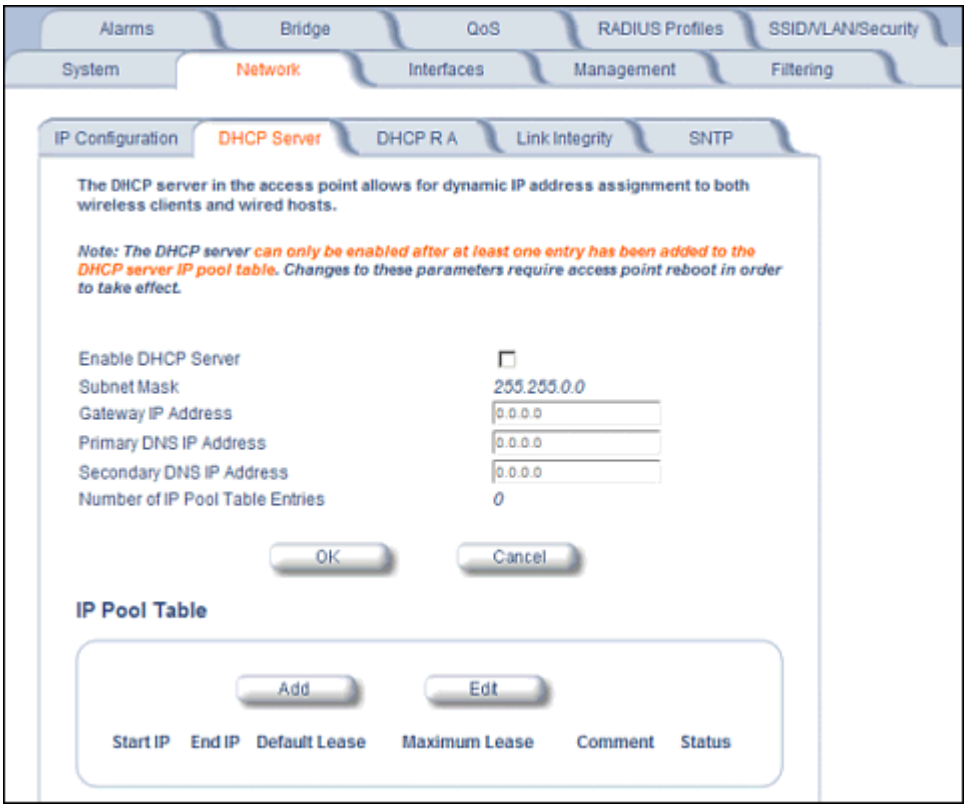


Figure 4-4 DHCP Server Configuration Screen

You can configure and view the following parameters within the ***DHCP Server Configuration*** screen:

NOTE: *You must reboot the Access Point before changes to any of these DHCP server parameters take effect.*

- **Enable DHCP Server:** Place a check mark in the box provided to enable DHCP Server functionality.

  NOTE: *You cannot enable the DHCP Server functionality unless there is at least one IP Pool Table Entry configured.*

- **Subnet Mask:** This field is read-only and reports the Access Point's current subnet mask. DHCP clients that receive dynamic addresses from the AP will be assigned this same subnet mask.
- **Gateway IP Address:** The AP will assign the specified address to its DHCP clients.
- **Primary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Secondary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Number of IP Pool Table Entries:** This is a read-only field that reports the number of entries in the IP Pool Table.
- **IP Pool Table Entry:** This entry specifies a range of IP addresses that the AP can assign to its wireless clients. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  - **Start IP Address**
  - **End IP Address**
  - **Default Lease Time (optional):** The default time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 0 and 86400 seconds. The default is 86400 seconds.
  - **Maximum Lease Time (optional):** The maximum time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 0 and 86400 seconds. The default is 86400 seconds.
  - **Comment (optional)**

– **Status:** IP Pools are enabled upon entry in the table. You can also disable or delete entries by changing this field's value.

NOTE: *You must reboot the Access Point before changes to any of these DHCP server parameters take effect.*

DHCP Relay Agent

When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server.

Click the **Configure > Network > DHCP R A** to configure DHCP relay agent servers and enable the DHCP relay agent.

NOTE: *At least one DHCP server must be enabled before DHCP Relay Agent can be enabled.*

The DHCP Relay functionality of the AP supports Option 82 and sends the system name of the AP (as a NAS identifier) as a sub-option of Option 82.

The AP makes a DHCP Request for lease renewal five minutes ahead of the expiration of the Rebinding time as specified in the DHCP Offer from the DHCP server obtained during the last renewal.

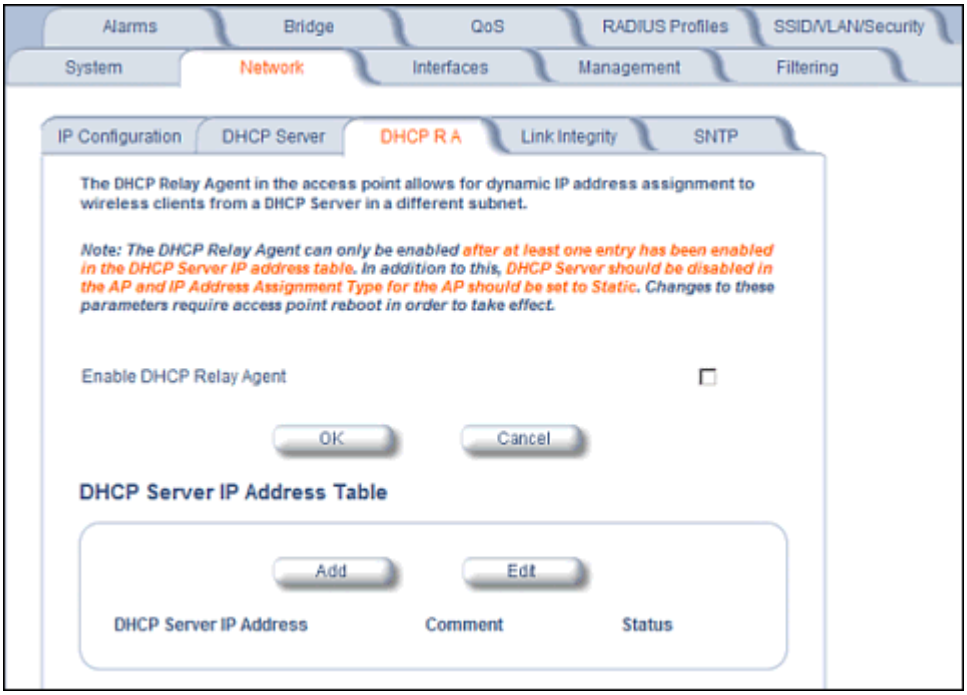


Figure 4-5 DHCP Relay Agent

DHCP Server IP Address Table

The AP supports the configuration of a maximum of 10 server settings in the DHCP Relay Agents server table. At least one server must be configured to enable DHCP Relay.

To add entries to the table of DHCP Relay Agents, click **Add** in the DHCP Server IP Address Table; to edit existing entries, click **Edit**. The following window is displayed.

Figure 4-6 DHCP Server IP Address Table - Edit Entries

To add an entry, enter the IP Address of the DHCP Server and a comment (optional), and click OK.

To edit an entry, make changes to the appropriate entry. Enable or disable the entry by choosing Enable or Disable from the Status drop-down menu, and click **OK**.

Link Integrity

The Link Integrity feature checks the link between the AP and the nodes on the Ethernet backbone. These nodes are listed by IP address in the Link Integrity IP Address Table. The AP periodically pings the nodes listed within the table. If the AP loses network connectivity (that is, the ping attempts fail), the AP disables its wireless interface(s). Note that this feature does not affect WDS links (if WDS links are configured and enabled).

NOTE: *Link integrity cannot be configured when the AP is configured to function as a Mesh AP.*

You can configure and view the following parameters within the ***Link Integrity Configuration*** screen:

- **Enable Link Integrity:** Place a check mark in the box provided to enable Link Integrity.
- **Poll Interval (milliseconds):** The interval between link integrity checks. Range is 500-15000 ms in increments of 500 ms; default is 500 ms.
- **Poll Retransmissions:** The number of times a poll should be retransmitted before the link is considered down. Range is 0 to 255; default is 5.
- **Target IP Address Entry:** This entry specifies the IP address of a host on the network that the AP will periodically poll to confirm connectivity. The table can hold up to five entries. By default, all five entries are set to 0.0.0.0. Click **Edit** to update one or more entries. Each entry contains the following field:
  - **Target IP Address**
  - **Comment (optional)**
  - **Status:** Set this field to **Enable** to specify that the Access Point should poll this device. You can also disable an entry by changing this field's value to **Disable**.

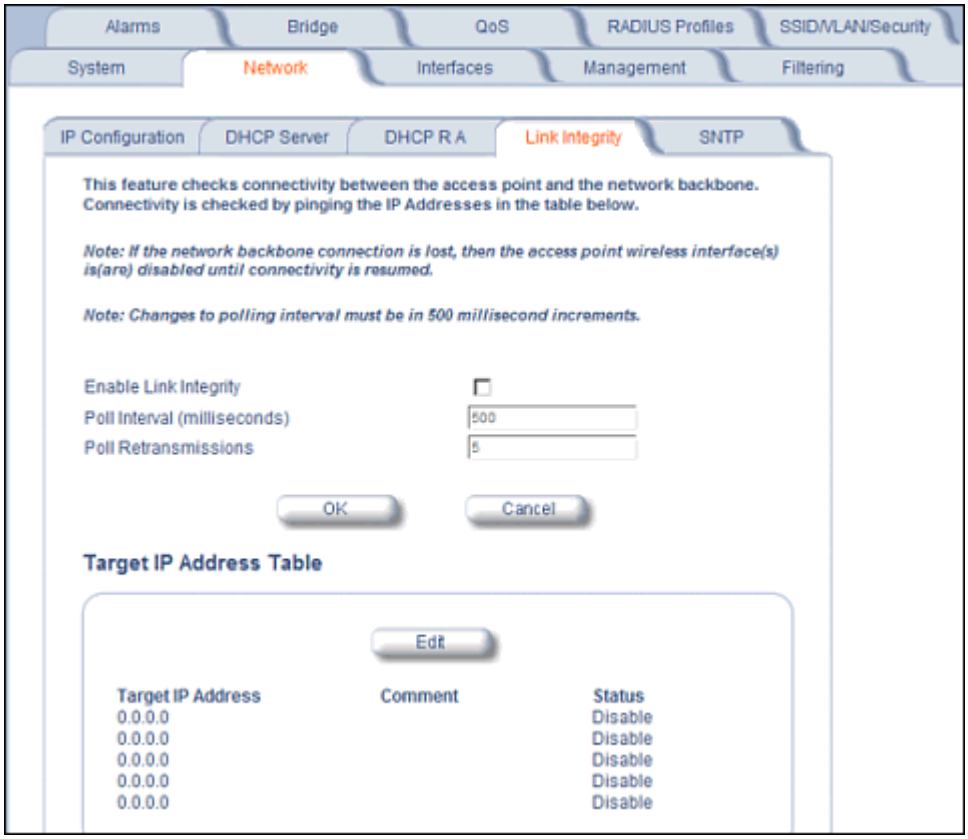


Figure 4-7 Link Integrity Configuration Screen

SNTP (Simple Network Time Protocol)

SNTP allows a network entity to communicate with time servers in the network/internet to retrieve and synchronize time of day information. When this feature is enabled, the AP will attempt to retrieve the time of day information from the configured time servers (primary or secondary), and, if successful, will update the relevant time objects in the AP. Requests are sent every 10 seconds. If the AP fails to retrieve the information after three attempts, the AP will use the system uptime and update the relevant time objects. If this feature is disabled, the user can manually configure the date and time parameters.

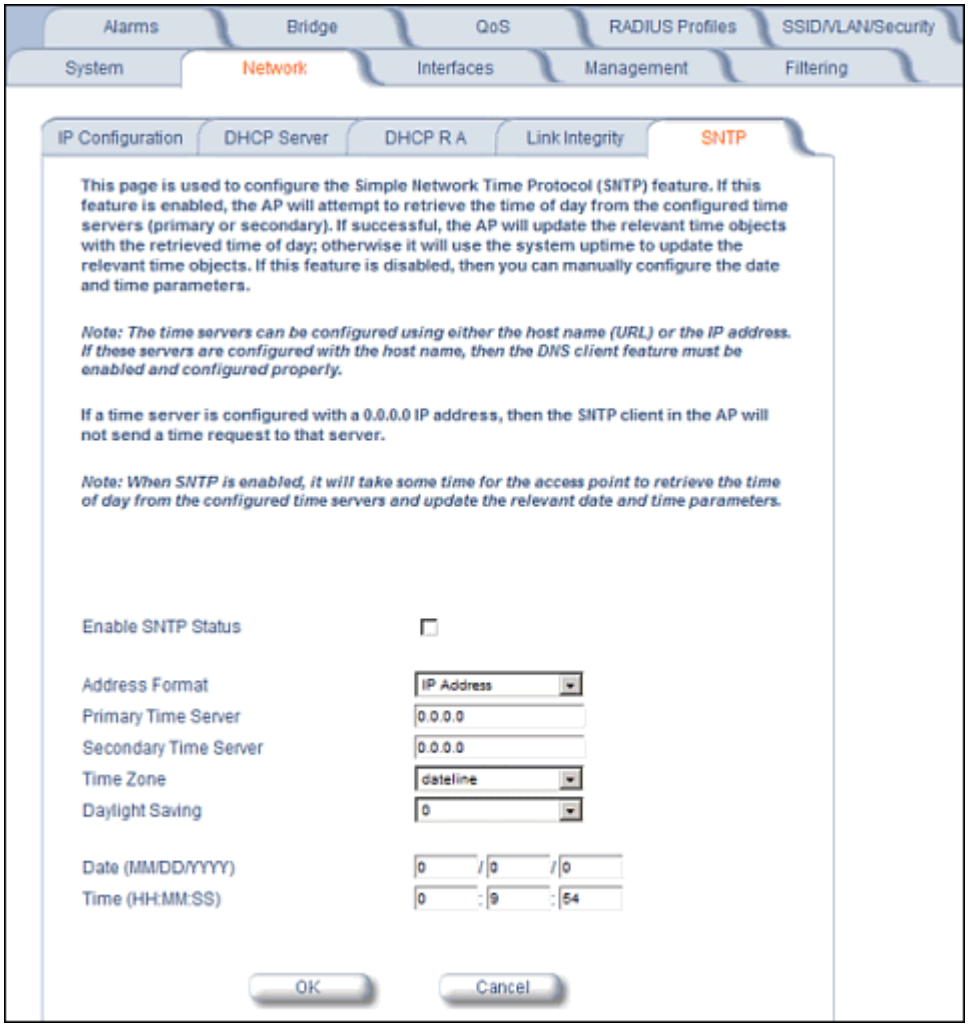


Figure 4-8 SNTP Configuration Screen

You can configure and view the following parameters within the SNTP screen:

- **SNTP Status**: Select Enable or Disable from the drop-down menu. The selected status will determine which of the parameters on the SNTP screen are configurable.

  NOTE: *When SNTP is enabled, it will take some time for the AP to retrieve the time of day from the configured time servers and update the relevant date and time parameters.*

- **Addressing Format**: If SNTP is enabled, choose whether you will use the host name or the IP address to configure the primary/secondary SNTP servers. If these servers are configured with the host name, the DNS client feature must be enabled and configured properly.
- **Primary Server Name or IP Address:** If SNTP is enabled, enter the host name or IP address of the primary SNTP server.
- **Secondary Server Name or IP Address**: If SNTP is enabled, enter the host name or IP address of the secondary SNTP server.
- Time Zone: Select the appropriate time zone from the drop down menu.
- **Daylight Savings Time:** Select the number of hours to adjust for daylight savings time.
- **Time and Date Information:** When SNTP is disabled, the following time-relevant objects are manually configurable. When SNTP is enabled, these objects are grayed out:

- Year: Enter the current year.
- Month: Enter the month in digits (1-12).
- Day: Enter the day in digits (1-31).
- Hour: Enter the hour in digits (0-23).
- Minutes: Enter the minutes in digits (0-59).
- Seconds: Enter the seconds in digits (0-59).

Interfaces

From the **Interfaces** tab, you configure the Access Point's operational mode settings, power control settings, wireless interface settings and Ethernet settings. You may also configure a Wireless Distribution System for AP-to-AP communications. The **Interfaces** tab contains the following sub-tabs:

- Operational Mode
- Wireless-A (802.11a Radio) and Wireless-B (802.11b/g Radio)
- Ethernet
- Mesh (AP-4000M/AP-4900M Only)

Operational Mode

From this tab, you can configure and view the operational mode for the Wireless-A (802.11a radio) or Wireless-B (802.11b/g radio) Interface.

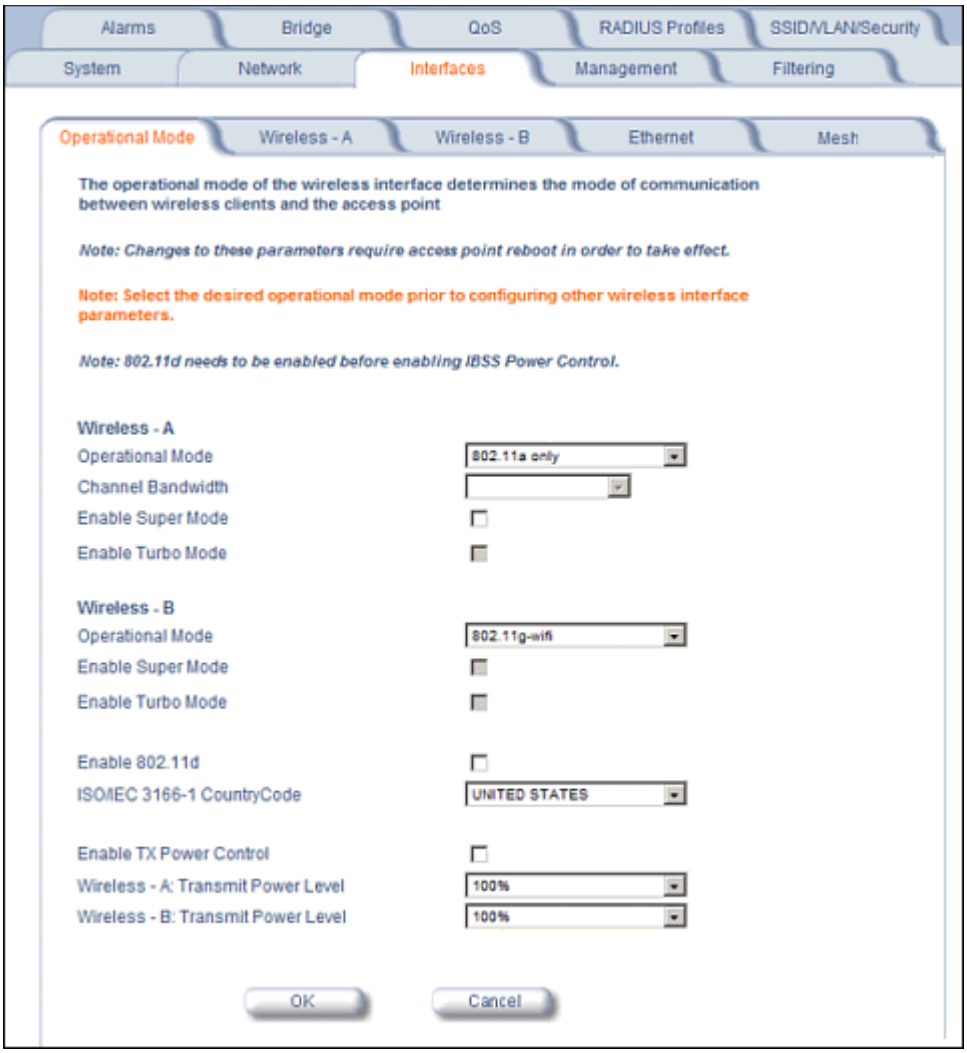


Figure 4-9 Operational Mode Screen (AP-4900M)

The Wireless-A interface operates only in 802.11a mode on the AP-4000/4000M and in either 802.11a mode or 4.9 GHz Public Safety mode on the AP-4900M. The Wireless-B interface can be configured to operate in the following modes:

- **802.11b only mode:** The radio uses the 802.11b standard only.

- **802.11g only mode:** The radio is optimized to communicate with 802.11g devices. This setting will provide the best results if this radio interface will only communicate with 802.11g devices.
- **802.11b/g mode:** This is the default mode. Use this mode if you want to support a mix of 802.11b and 802.11g devices.
- **802.11g-wifi mode:** The 802.11g-wifi mode has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

In general, you should use either 802.11g only mode (if you want to support 802.11g devices only) or 802.11b/g mode to support a mix of 802.11b and 802.11g devices.

If you are using the AP-900 and 4.9 Public Safety mode, you must also select a channel bandwidth. This option is shown in Figure 4-9; it is not available in the AP-4000/4000M. See Available Channels for a list of channels available with each bandwidth.

Super Mode and Turbo Mode

Super mode improves throughput between the access point and wireless clients that support this capability. For wireless clients that support this capability the AP will negotiate and treat them accordingly, for other clients that do not support super mode, the AP will treat them as normal wireless clients.

Super mode can be configured only when the wireless operational mode is one of the following:

- 802.11a only mode
- 802.11g only mode
- 802.11b/g mode

NOTE: *Super mode and Turbo mode are not available in operational modes 802.11b and 802.11g-wifi.*

Dynamic Turbo mode is supported in 802.11a and 802.11g mode. Dynamic turbo mode supports turbo speeds at twice the standard 802.11a/g data rates, and also dynamically switches between turbo mode speeds and normal speeds depending on the wireless client. If turbo mode is enabled, then this is displayed in the web UI and the transmit speeds and channels pull-down menus are updated with the valid values.

When Turbo mode is enabled, only a subset of the wireless channels on both the 2.4 GHz and 5.0 GHz spectrum can be used. If any wireless clients do not support turbo mode, the AP will fall back to normal mode.

Turbo mode can be configured only when Super mode has already been enabled.

Super mode is supported in the 2.4 GHz and 5 GHz frequency bands in all regulatory domains. Turbo mode is available in the 5 GHz frequency band in all regulatory domains except for Japan.

NOTE: *Turbo mode and Mesh mode (either Mesh AP or Mesh Portal) can not be enabled on the same interface simultaneously.*

IEEE 802.11d Support for Additional Regulatory Domains

The IEEE 802.11d specification allows conforming equipment to operate in more than one regulatory domain over time. IEEE 802.11d support allows the AP to broadcast its radio's regulatory domain information in its beacon and probe responses to clients. This allows clients to passively learn what country they are in and only transmit in the allowable spectrum. When a client enters a regulatory domain, it passively scans to learn at least one valid channel, i.e., a channel upon which it detects IEEE Standard 802.11 frames.

The beacon frame contains information on the country code, the maximum allowable transmit power, and the channels to be used for the regulatory domain.

The same information is transmitted in probe response frames in response to a client's probe requests. Once the client has acquired the information required to meet the transmit requirements of the regulatory domain, it configures itself for operation in the regulatory domain.

The Wireless NIC determines the regulatory domain the AP is operating in. If the AP has dual Wireless NICs, the NIC in Slot A determines the regulatory domain. Depending on the regulatory domain, a default country code is chosen that is transmitted in the beacon and probe response frames.

Configuring 802.11d Support

Perform the following procedure to enable 802.11d support and select the country code:

1. Click **Configure > Interfaces > Operational Mode**.
2. Select **Enable 802.11d**.
3. Select the Country Code from the ISO/IEC 3166-1 CountryCode drop-down menu.
4. Click **OK**.
5. Configure Transmit Power Control and transmit power level if required.

TX Power Control/Transmit Power Level

Transmit Power Control uses standard 802.11d frames to control transmit power within an infrastructure BSS. This method of power control is considered to be an interim way of controlling the transmit power of 802.11d enabled clients in lieu of implementation of 802.11h.

The Transmit Power Control feature lets the user configure the transmit power level of the wireless interface at one of four levels:

- 100% of the maximum transmit power level defined by the regulatory domain
- 50%
- 25%
- 12.5%

When Transmit Power Control is enabled, the transmit power level of the card in the AP is set to the configured transmit power level. The power level is advertised in Beacon and Probe Response frames as the 802.11d maximum transmit power level.

When an 802.11d-enabled client learns the regulatory domain related information from Beacon and Probe Response frames, it learns the power level advertised in Beacon and Probe response frames as the maximum transmit power of the regulatory domain and configures itself to operate with that power level.

As a result, the transmit power level of the BSS is configured to the power level set in the AP (assuming that the BSS has only 802.11d enabled clients and an 802.11d enabled AP).

Configuring TX Power Control

1. Click **Configure > Interfaces > Operational Mode**.
2. Select **Enable Transmit Power Control**.
3. Select the transmit power level for wireless interface A or B from the Wireless-A or Wireless-B: Transmit Power Level drop-down menu.
4. Click **OK**.

Wireless-A (802.11a Radio) and Wireless-B (802.11b/g Radio)

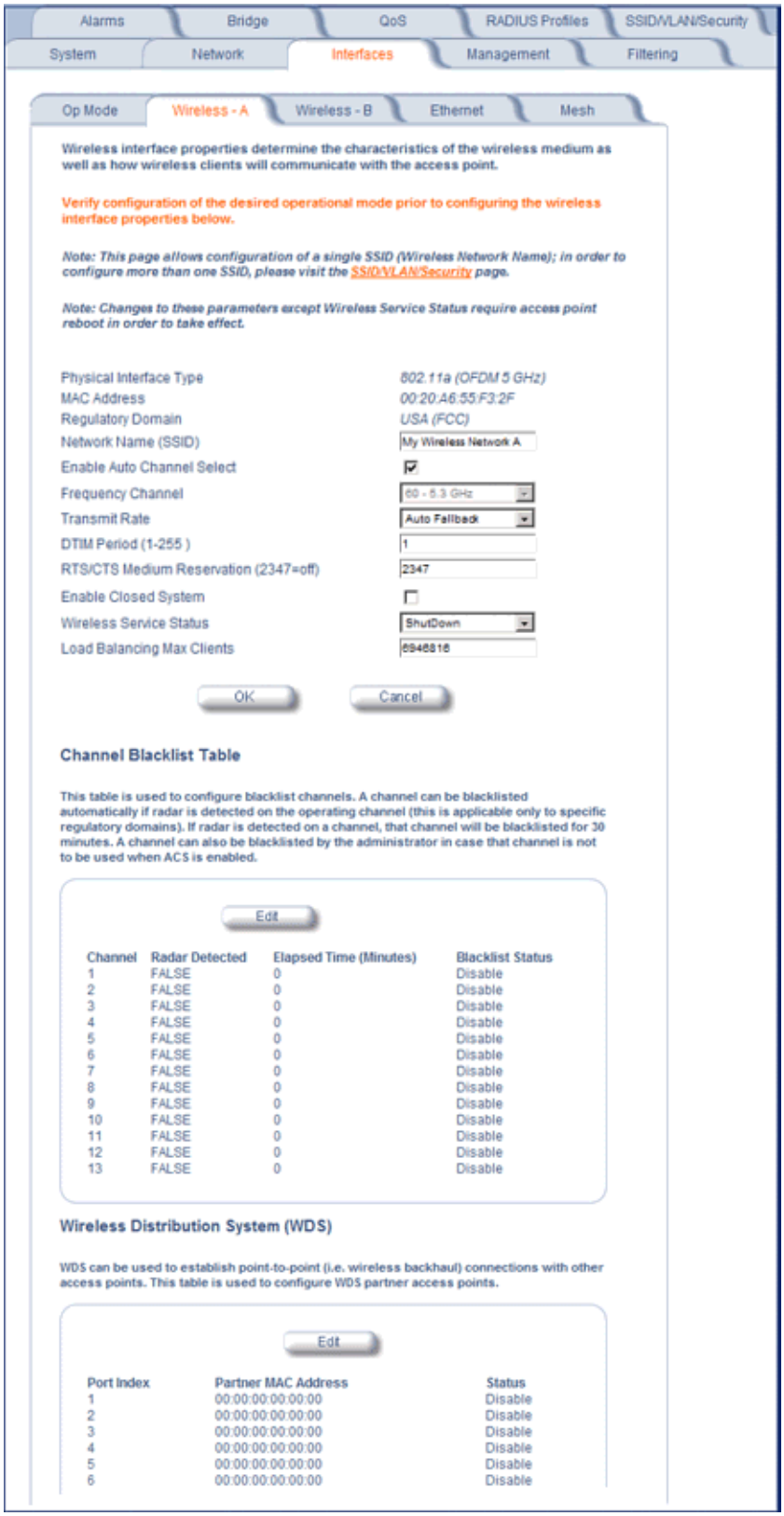


Figure 4-10 Wireless Interface A

You can view and configure the following parameters for the Wireless-A and Wireless-B interfaces:

NOTE: *You must reboot the Access Point before any changes to these parameters take effect.*

- **Physical Interface Type:** For Wireless Interface A on the AP-4000/4000M, this field reports “802.11a (OFDM 5 GHz)”. On the AP-4900M, this field reports “802.11a (OFDM 5 GHz)” when operating in 802.11a only mode or “Public Safety (OFDM 4.9 GHz)” when operating in 4.9 GHz Public Safety mode. For Wireless Interface B on the AP-4000/4000M/4900M, depending on the operational mode, this field reports:
  – For 802.11b mode only: "802.11b (DSSS 2.4 GHz)"
  – For 802.11g mode: "802.11g (OFDM/DSSS 2.4 GHz)"
  – For 802.11b/g mode: "802.11g (OFDM/DSSS 2.4 GHz)"
  – For 802.11g-wifi mode: "802.11g (OFDM/DSSS 2.4 GHz)"

  NOTE: *802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.*

  OFDM stands for Orthogonal Frequency Division Multiplexing; this is the name for the radio technology used by 802.11a devices. DSSS stands for Direct Sequence Spread Spectrum; this is the name for the radio technology used by 802.11b devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point’s wireless interface. The MAC address is assigned at the factory.
- **Regulatory Domain:** Reports the regulatory domain for which the AP is certified. Not all features or channels are available in all countries.
- **Network Name (SSID):** Enter a Network Name (between 1 and 32 characters long) for the primary wireless network. You must configure each wireless client using this network to use this name as well. Additional SSIDs and VLANs may be configured under **Configure** > **SSID/VLAN/Security**. Up to 16 SSID/VLANs may be configured per wireless interface.

  NOTE: *Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.*
- **Auto Channel Select:** The AP scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled. See Dynamic Frequency Selection/Radar Detection (DFS/RD) for more information and Available Channels for a list of available channels.

  NOTE: *When an AP is configured to function as a Mesh AP, its channel will depend on the channel of its neighbors.*
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point’s current operating Channel. When Auto Channel Select is disabled, you can specify the Access Point’s operating channel. If you decide to manually set the unit’s Channel, ensure that nearby devices do not use the same frequency (unless you are setting up WDS links). Available channels vary based on regulatory domain. See Dynamic Frequency Selection/Radar Detection (DFS/RD) for more information and Available Channels for a list of available channels.

  NOTE: *When an AP is configured to function as a Mesh AP, its channel will depend on the channel of its neighbors.*
- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP. The values depend on the Operational mode. Auto Fallback is the default setting; it allows the AP unit to select the best transmit rate based on the cell size.
  – For 802.11a only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s.
  – For 4.9 GHz Public Safety mode, the transmit rate depends on the channel bandwidth selected:
    — For operation in 10 MHz bandwidth: Auto Fallback, 3, 4.5, 6, 9, 12, 18, 24, 27 Mbits/s.
    — For operation in 20 MHz bandwidth: Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s.
  – For 802.11b only -- Auto Fallback, 1, 2, 5.5, 11 Mbits/sec.
  – For 802.11g only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/sec

  - For 802.11b/g -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec
  - For 802.11g-wifi -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec

  NOTE: *802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.*

  NOTE: *Turbo mode is supported in 802.11a and 802.11g mode. If turbo mode is enabled, then this is displayed in the web UI and the transmit speeds and channels pull-down menus are updated with the valid values.*

- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) Period determines when to transmit broadcast and multicast packets to all clients. If any clients are in power save mode, packets are sent at the end of the DTIM period. This parameter supports a range between 1 and 255; it is recommended to leave the DTIM at its default value unless instructed by technical support. Higher values conserve client battery life at the expense of network performance for broadcast or multicast traffic.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See RTS/CTS Medium Reservation for more information.
- **Enable Closed System:** When enabled, the AP will not respond to probe requests from client stations requesting “ANY.” Enabling closed system will require the client station to configure the SSID of the AP manually.
- **Wireless Service Status**: Select **Shutdown** to shutdown the wireless service on a wireless interface, or resume to resume wireless service. See Wireless Service Status for more information.
- **Load Balancing Max Clients**: Load balancing distributes clients among available access points. Enter a number between 1 and 63 to specify the maximum number of clients to allow.
- **Channel Blacklist Table**: The Channel Blacklist table contains all available channels. It can be used to manually blacklist channels, and it also reflects channels that have been automatically blacklisted by the Dynamic Frequency Selection/Radar Detection (DFS/RD) function. See Channel Blacklist Table for configuration information.
- **Wireless Distribution System**: A Wireless Distribution system can be used to establish point-to-point (i.e. wireless backhaul) connections with other access points. See Wireless Distribution System (WDS) for configuration information.

Dynamic Frequency Selection/Radar Detection (DFS/RD)

In order to prevent interference with radar systems and other devices that occupy the 5 GHz band, 802.11a APs certified in the ETSI (Europe) and TELEC (Japan) regulatory domains (see Affected Countries) and operating in the middle frequency band select an operating channel through a combination of Auto Channel Select (ACS) and Dynamic Frequency Selection (DFS)/Radar Detection (RD).

During boot-up, ACS scans the available channels and selects the best channel. Once a channel is selected, the AP performs a channel availability check for 60 seconds to ensure that there is no radar on the channel and then commences normal operation. When the AP enters normal operation, DFS works in the background to detect radar interference on that channel. If interference is detected, the AP sends a trap, disassociates all clients, blacklists the channel, and reboots. After it reboots, ACS re-scans and selects a better channel that is free of interference.

If ACS is disabled, only channels in the lower frequency band are available for use:

- 36: 5.18 GHz (default)
- 40: 5.200 GHz
- 44: 5.220 GHz
- 48: 5.240 GHz

Affected Countries

Japan is certified in the TELEC regulatory domain for operation in the 5 GHz band. The following countries are certified in the ETSI regulatory domain for operation in the 5 GHz band:

- Austria
- Belgium
- Brazil
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Iceland
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Saudi Arabia
- Spain
- Sweden
- Switzerland
- UK

RTS/CTS Medium Reservation

The 802.11 standard supports optional RTS/CTS communication based on packet size. Without RTS/CTS, a sending radio listens to see if another radio is already using the medium before transmitting a data packet. If the medium is free, the sending radio transmits its packet. However, there is no guarantee that another radio is not transmitting a packet at the same time, causing a collision. This typically occurs when there are hidden nodes (clients that can communicate with the Access Point but are out of range of each other) in very large cells.

When RTS/CTS occurs, the sending radio first transmits a Request to Send (RTS) packet to confirm that the medium is clear. When the receiving radio successfully receives the RTS packet, it transmits back a Clear to Send (CTS) packet to the sending radio. When the sending radio receives the CTS packet, it sends the data packet to the receiving radio. The RTS and CTS packets contain a reservation time to notify other radios (including hidden nodes) that the medium is in use for a specified period. This helps to minimize collisions. While RTS/CTS adds overhead to the radio network, it is particularly useful for large packets that take longer to resend after a collision occurs.

RTS/CTS Medium Reservation is an advanced parameter and supports a range between 0 and 2347 bytes. When set to 2347 (the default setting), the RTS/CTS mechanism is disabled. When set to 0, the RTS/CTS mechanism is used for all packets. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. You should not need to enable this parameter for most networks unless you suspect that the wireless cell contains hidden nodes.

Wireless Service Status

The user can shut down (or resume) the wireless service on the wireless interface of the AP through the CLI, HTTP, or SNMP interface. When the wireless service on a wireless interface is shut down, the AP will:

- Stop the AP services to wireless clients connected on that wireless interface by disassociating them
- Disable the associated BSS ports on that interface
- Disable the transmission and reception of frames on that interface
- Indicate the wireless service shutdown status of the wireless interface through LED and traps
- Enable Ethernet interface so that it can receive a wireless service resume command through CLI/HTTP/SNMP interface

NOTE: *WSS disables BSS ports.*

NOTE: *The wireless service cannot be shutdown on an interface where Rogue Scan is enabled.*

In shutdown state, AP will not transmit and receive frames from the wireless interface and will stop transmitting periodic beacons. Moreover, none of the frames received from the Ethernet interface will be forwarded to that wireless interface.

Wireless service on a wireless interface of the AP can be resumed through CLI/HTTP/SNMP management interface. When wireless service on a wireless interface is resumed, the AP will:

- Enable the transmission and reception of frames on that wireless interface
- Enable the associated BSS port on that interface
- Start the AP services to wireless clients
- Indicate the wireless service resume status of the wireless interface through LED and traps

After wireless service resumes, the AP resumes beaconing, transmitting and receiving frames to/from the wireless interface and bridging the frames between the Ethernet and the wireless interface.

Traps Generated During Wireless Service Shutdown (and Resume)

The following traps are generated during wireless service shutdown and resume, and are also sent to any configured Syslog server.

When the wireless service is shut down on a wireless interface, the AP generates a trap called *oriTrapWirelessServiceShutdown*.

When the wireless service is resumed on a wireless interface, the AP generate a trap called *oriTrapWirelessServiceResumed*.

Channel Blacklist Table

The Channel Blacklist table contains all available channels (channels vary based on regulatory domain). It can be used to manually blacklist channels, and it also reflects channels that have been automatically blacklisted by the Dynamic Frequency Selection/Radar Detection (DFS/RD) function. In the ETSI (Europe) and TELEC (Japan) regulatory domains, channels are blacklisted automatically when radar is detected; when a channel has been automatically blacklisted, the Radar Detected status is set to True, and the channel will remain remain blacklisted for 30 minutes. Additionally, an administrator can blacklist channels manually to prevent their being used when ACS is enabled. To blacklist a channel manually:

1. Click on **Configure** > **Interfaces** > **Wireless A** or **Wireless B**.
2. Scroll down to the **Channel Blacklist** heading.

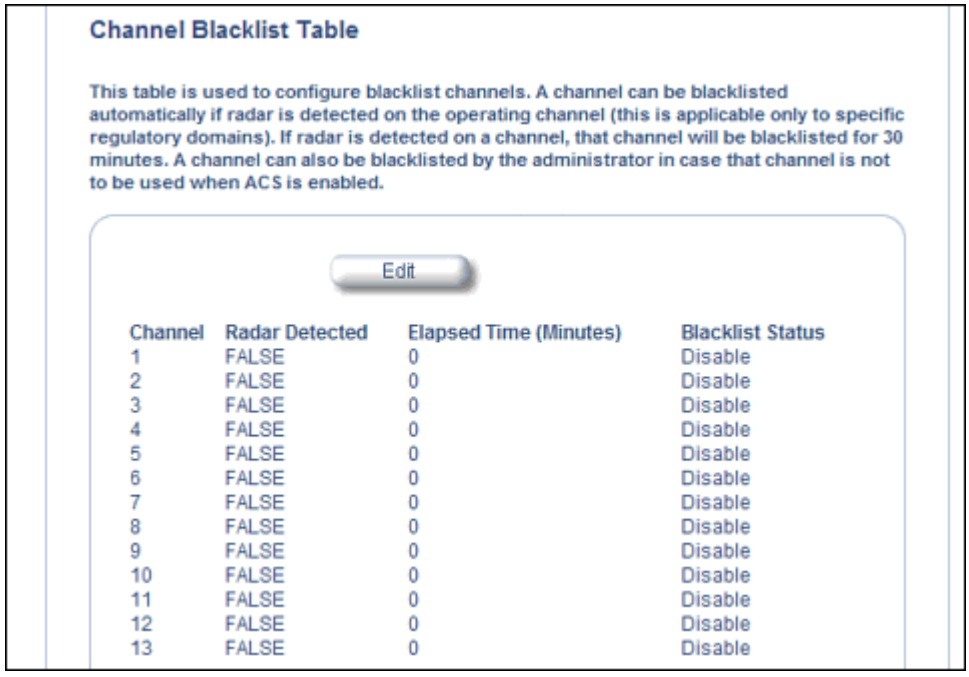


Figure 4-11 Channel Blacklist Table

3. Click **Edit** in the Channel Blacklist Table

4. Set **Blacklist Status** to **Enable**.

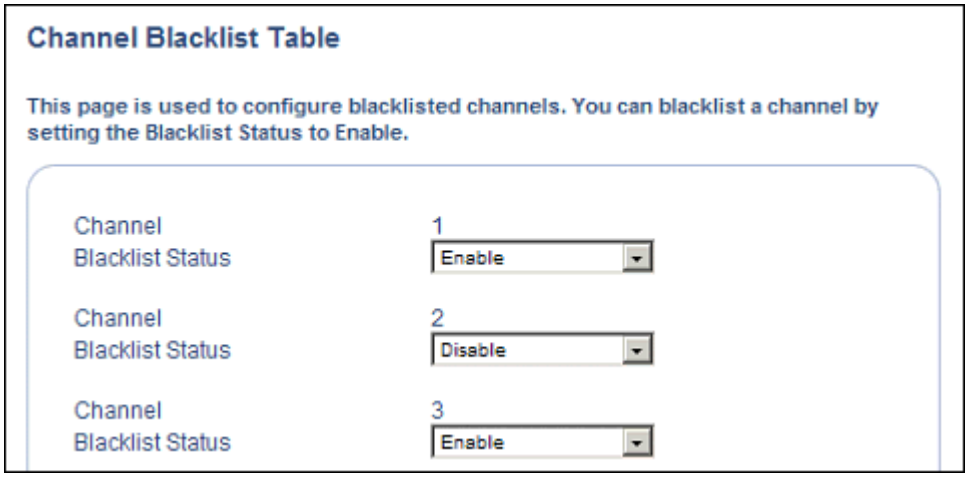


Figure 4-12 Channel Blacklist Table - Edit Screen

NOTE: *In the AP-4000/4000M/4900M, wireless service can be shut down/resumed on each wireless interface individually.*

Wireless Distribution System (WDS)

A Wireless Distribution System (WDS) creates a link between two 802.11a, 802.11b, or 802.11b/g APs over their radio interfaces. This link relays traffic from one AP that does not have Ethernet connectivity to a second AP that has Ethernet connectivity. WDS allows you to configure up to six (6) ports per radio, or up to 12 ports on the AP-4000/4000M/4900M.

In the WDS example below, AP 1 and AP 2 communicate over a WDS link (represented by the blue line). This link provides Client 2 with access to network resources even though AP 2 is not directly connected to the Ethernet network. Packets destined for or sent by the client are relayed between the Access Points over the WDS link.

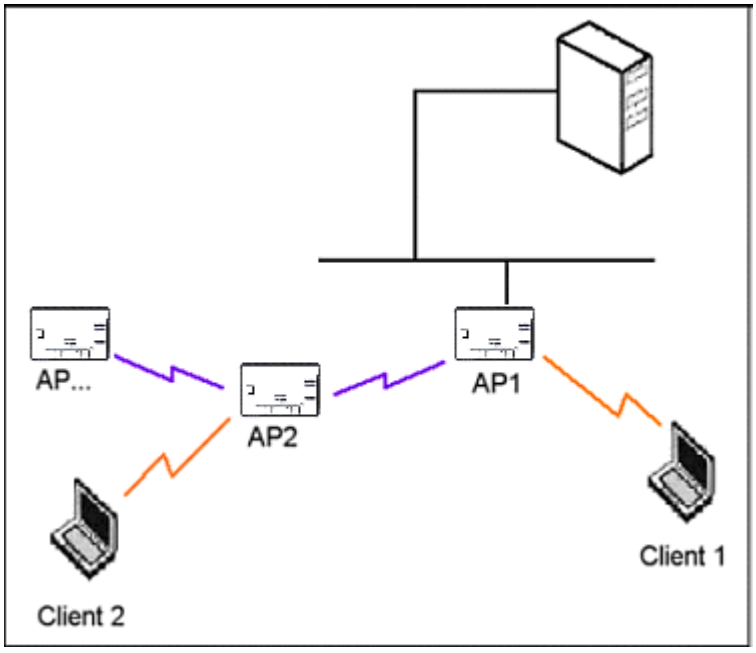


Figure 4-13 WDS Example

Bridging WDS

Each WDS link is mapped to a logical WDS port on the AP. WDS ports behave like Ethernet ports rather than like standard wireless interfaces: on a BSS port, an Access Point learns by association and from frames; on a WDS or Ethernet port, an Access Point learns from frames only. When setting up a WDS, keep in mind the following:

- WDS and Mesh functionality cannot be enabled on the same radio when the AP is configured to function as a Mesh AP.
- There are separate security settings for clients and WDS links. The same WDS link security mode must be configured (currently we only support none or WEP) on each Access Point in the WDS and the same WEP key must be configured.
- The WDS link shares the communication bandwidth with the clients. Therefore, while the maximum data rate for the Access Point's cell is 54 Mbits/second (802.11a, 802.11g only, or 802.b/g modes) or 11 Mbits/second (802.11b only mode), client throughput will decrease when the WDS link is active.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- Each WDS port on a single AP should have a unique partner MAC address. Do not enter the same MAC address twice in an AP's WDS port list.
- Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.
- If your network does not support spanning tree, be careful to avoid creating network loops between APs. For example, creating a WDS link between two Access Points connected to the same Ethernet network will create a network loop (if spanning tree is disabled). For more information, see the Spanning Tree section.

WDS Setup Procedure

NOTE: *You must disable Auto Channel Select to create a WDS. Each Access Point that is a member of the WDS must have the same channel setting to communicate with each other.*

NOTE: *WDS and Mesh functionality cannot be enabled on the same radio when the AP is configured to function as a Mesh AP.*

To setup a wireless backbone follow the steps below for each AP that you wish to include in the Wireless Distribution System.

1. Confirm that Auto Channel Select is disabled.
2. Write down the MAC Address of the radio that you wish to include in the Wireless Distribution System.
3. Click on **Configure** > **Interfaces** > **Wireless A** or **Wireless B**.
4. Scroll down to the **Wireless Distribution System** heading.

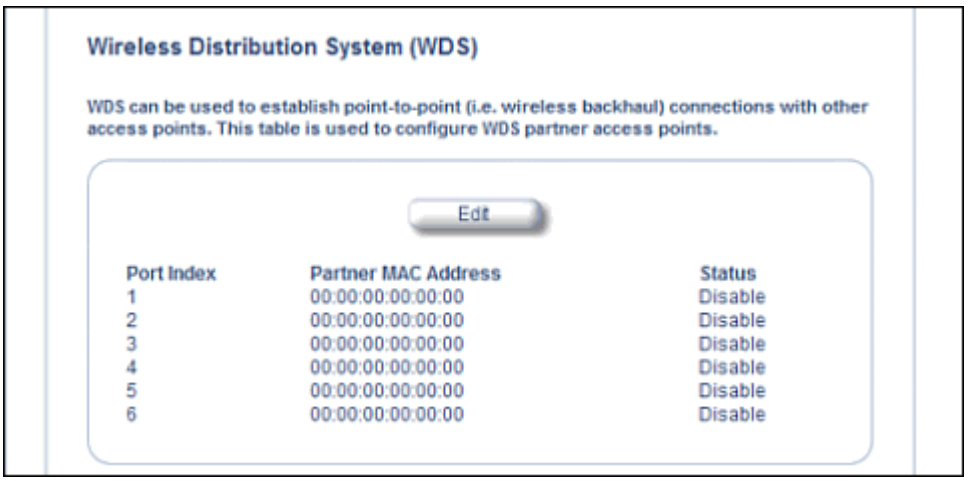


Figure 4-14 WDS Configuration

5. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.

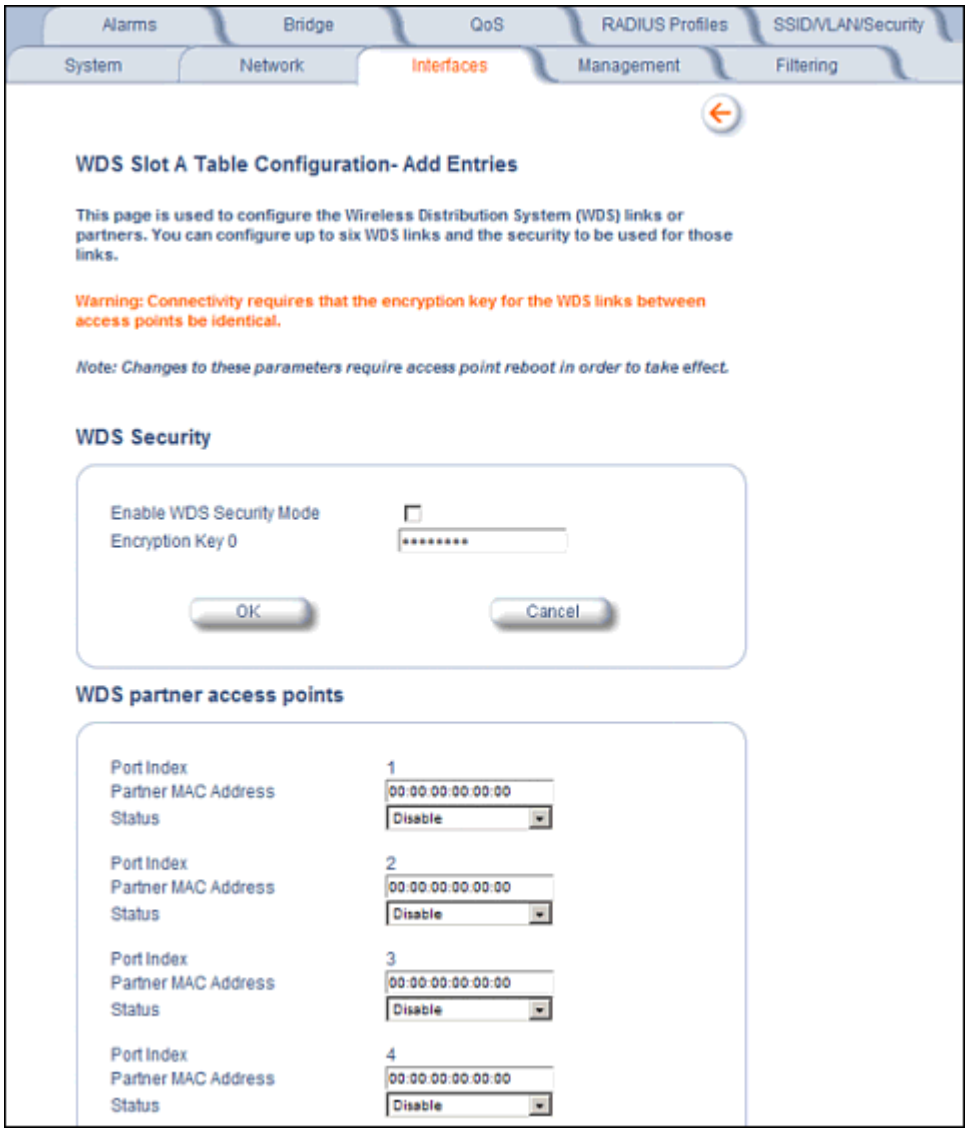


Figure 4-15 Adding WDS Links

6. Select whether to use encryption in the WDS by checking the **Enable WDS Security Mode** checkbox.
7. If you enabled WDS Security Mode, enter the **Encryption Key 0** used for encryption between the WDS links.
8. Enter the MAC Address that you wrote down in Step 2 in one of the **Partner MAC Address** field of the Wireless Distribution Setup window.
9. Set the **Status** of the device to **Enable**.
10. Click **OK**.
11. Reboot the AP.

Ethernet

Select the desired speed and transmission mode from the drop-down menu. Half-duplex means that only one side can transmit at a time and full-duplex allows both sides to transmit. When set to auto-duplex, the AP negotiates with its switch or hub to automatically select the highest throughput option supported by both sides.

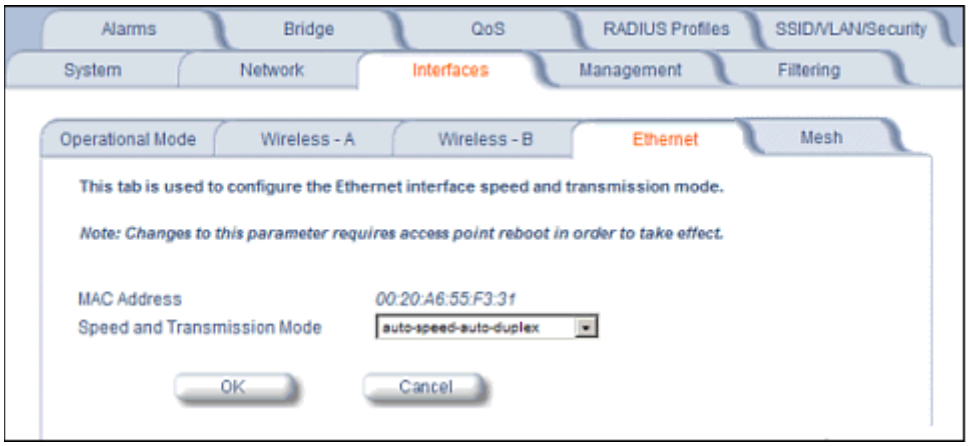


Figure 4-16 Ethernet Sub-tab

For best results, Proxim recommends that you configure the Ethernet setting to match the speed and transmission mode of the device the Access Point is connected to (such as a hub or switch). If in doubt, leave this setting at its default, **auto-speed-auto-duplex**. Choose between:

- 10 Mbit/s - half duplex or full duplex
- 100 Mbit/s - half duplex or full duplex
- Auto speed - auto duplex

Mesh (AP-4000M/AP-4900M Only)

Mesh functionality can be enabled on only one of the AP's wireless interfaces. When configured for Mesh, the AP's wireless interface simultaneously functions as a mesh link and as a radio to service clients.

Mesh is available only the AP-4000M and AP-4900M models. To convert an AP-4000 to an AP-4000M and enable Mesh capabilities, see Mesh Software Kit.

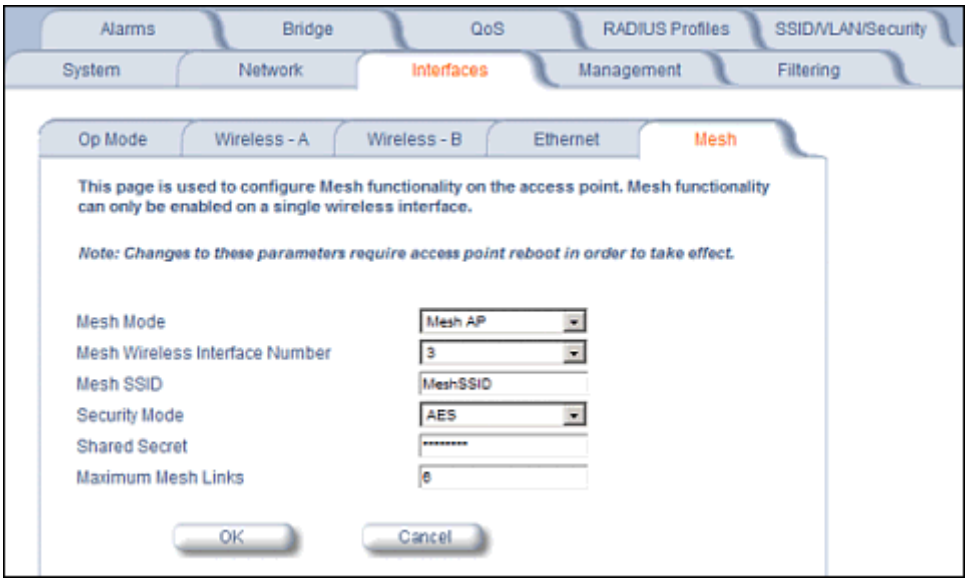


Figure 4-17 Mesh Sub-tab (AP-4000M/AP-4900M)

The following parameters are used to configure Mesh functionality on the access point.

CAUTION: *Mesh mis-configuration may cause problems in your wireless network. Before configuring an interface for Mesh functionality, see* Mesh Network Configuration.

NOTE: *Changes to these parameters require a reboot in order to take effect.*

- **Mesh Mode:** Use this drop down menu to enable/disable Mesh functionality on a wireless interface. When Mesh Mode is set to Disable, all other parameters on this tab will be grayed out. To enable Mesh functionality, choose one of the following:
  - **Mesh Portal:** Choose this option if the AP will be connected directly to the wired backbone.
  - **Mesh AP:** Choose this option if the AP will connect to the portal and backbone wirelessly.
- **Mesh Wireless Interface Number:** Select the wireless interface on which to enable Mesh functionality. Select 3 for Wireless Interlace A (802.11a radio) or 4 for Wireless Interface B (802.11b/g radio).
- **Mesh SSID:** Enter a unique Mesh Network Name (SSID) between 1 and 16 characters.

  NOTE: *Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.*
- **Security Mode:** Select **None** to use Mesh networking without security, or **AES** to enable AES encryption between Mesh links.
- **Shared Secret:** Enter a password between 6 and 32 characters. This is the password shared between Mesh APs and Portals when AES is selected as the security mode.
- **Maximum Mesh Links:** Select a number between 1 and 6 to configure the number of mesh links that can be connected to a single Mesh portal or Mesh AP, as follows:
  - For a Mesh Portal, up to six downlink connections are supported. Proxim recommends a maximum of 20-30 APs per portal. See Mesh Network Configuration.

– For a Mesh AP, one uplink and up to 5 downlink connections are supported.

For more information on Mesh, see Mesh Networking (AP-4000M/4900M Only).

Mesh Software Kit

The Mesh Software Kit (purchased seperately) converts an AP-4000 unit into an AP-4000M unit that supports Mesh capabilities. To covert your AP using the Mesh Software Kit, follow the steps below:

1. Print the Mesh sub-tab page containing all the necessary conversion information: software version, serial number, Ethernet MAC address, and security ID.

Figure 4-18 Mesh Sub-tab (AP-4000)

2. Contact your VAR or sales representative. You will be asked for the information obtained in step 1 above. Follow the instructions provided by your VAR or sales representative to obtain the Mesh Software Kit for conversion.
3. Update the AP with the license file included in the Mesh Software Kit. See Update AP via TFTP or Update AP via HTTP.
4. Reboot the AP. When the AP reboots, Mesh capabilities will be supported, and the AP can be configured to operate in a Mesh network.
5. See the Mesh (AP-4000M/AP-4900M Only) section above to configure Mesh networking.

Management

The Management tab contains the following sub-tabs:

- Passwords
- IP Access Table
- Services
- Automatic Configuration (AutoConfig)
- Hardware Configuration Reset (CHRD)

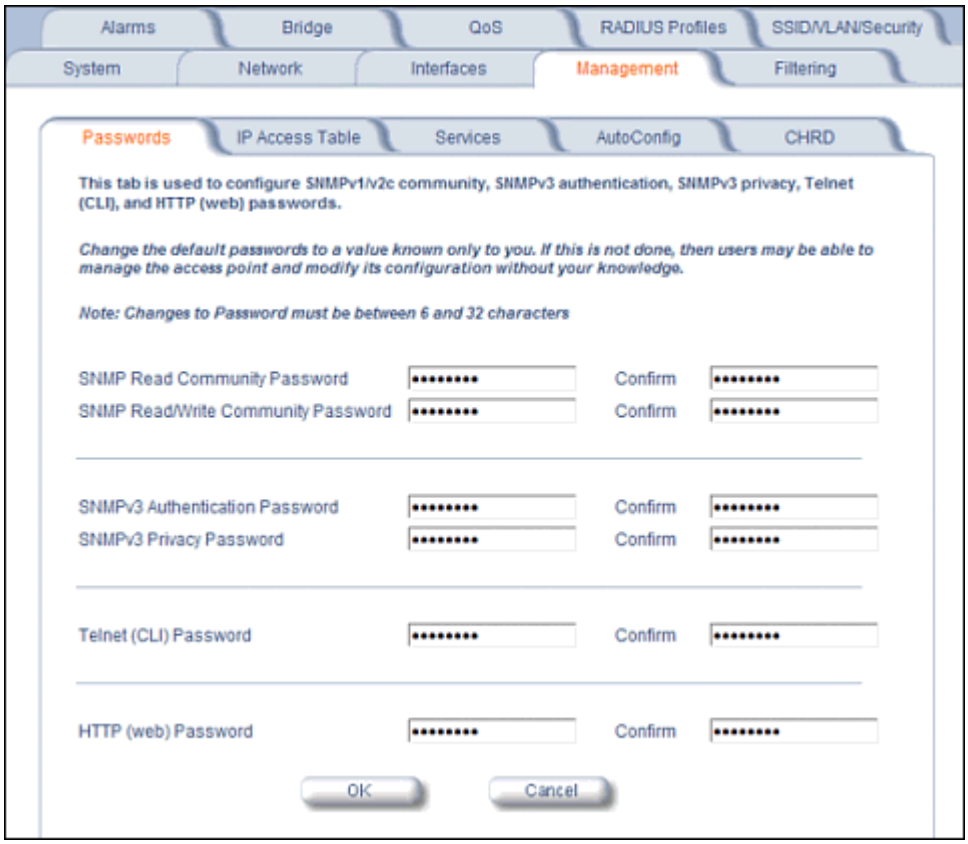
Passwords

You can configure the following passwords:

- **SNMP Read Community Password:** The password for read access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters. The default password is “public”.
- **SNMP Read/Write Community Password:** The password for read and write access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters. The default password is “public”.
- **SNMPv3 Authentication Password:** The password used when sending authenticated SNMPv3 messages. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters, but a length of at least 8 characters is recommended. The default password is “public”. Secure Management (Services tab) must be enabled to configure SNMPv3.

  The default SNMPv3 username is **administrator**, with SHA authentication and DES privacy protocol.
- **SNMPv3 Privacy Password:** The password used when sending encrypted SNMPv3 data. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters, but a length of at least 8 characters is recommended. The default password is “public”. Secure Management (Services tab) must be enabled to configure SNMPv3.
- **Telnet (CLI) Password:** The password for the CLI interface (via serial or Telnet). Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters. The default password is “public”.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters. The default password is “public”.

NOTE: *For security purposes Proxim recommends changing ALL PASSWORDS from the default “public” immediately, to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the* Reset to Factory Default Procedure*.*



IP Access Table

The Management IP Access table limits in-band management access to the IP addresses or range of IP addresses specified in the table. This feature applies to all management services (SNMP, HTTP, and CLI) except for CLI management over the serial port. To configure this table, click **Add** and set the following parameters:

- **IP Address:** Enter the IP Address for the management station.
- **IP Mask:** Enter a mask that will act as a filter to limit access to a range of IP Addresses based on the IP Address you already entered.
  - The IP mask 255.255.255.255 would authorize the single station defined by the IP Address to configure the Access Point. The AP would ignore commands from any other IP address. In contrast, the IP mask 255.255.255.0 would allow any device that shares the first three octets of the IP address to configure the AP. For example, if you enter an IP address of 10.20.30.1 with a 255.255.255.0 subnet mask, any IP address between 10.20.30.1 and 10.20.30.254 will have access to the AP's management interfaces.
- **Comment:** Enter an optional comment, such as the station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

Services

You can configure the following management services:

Secure Management

Secure Management allows the use of encrypted and authenticated communication protocols such as SNMPv3, Secure Socket Link (SSL), and Secure Shell (SSH) to manage the Access Point.

- **Secure Management Status:** Enables the further configuration of HTTPS Access, SNMPv3, and Secure Shell (SSH). After enabling Secure Management, you can choose to configure HTTPS (SSL) and Secure Shell access on the Services tab, and to configure SNMPv3 passwords on the Passwords tab.

SNMP Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**Ethernet**, **Wireless-Slot A, Wireless-Slot B**, **All Interfaces**) from which you will manage the AP via SNMP. You can also select **Disabled** to prevent a user from accessing the AP via SNMP.

HTTP Access

- **HTTP Interface Bitmap:** Configure the interface or interfaces (**Ethernet**, **Wireless-Slot A, Wireless-Slot B**, **All Interfaces**) from which you will manage the AP via the Web interface. For example, to allow Web configuration via the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the AP from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the AP via the Web interface. By default, the HTTP port is 80. You must reboot the Access Point if you change the HTTP Port.
- **HTTP Wizard Status:** The Setup Wizard appears automatically the first time you access the HTTP interface. If you exited out of the Setup Wizard and want to relaunch it, enable this option, click **OK**, and then close your browser or reboot the AP. The Setup Wizard will appear the next time you access the HTTP interface.

HTTPS Access (Secure Socket Layer)

NOTE: *SSL requires Internet Explorer version 6, 128 bit encryption, Service Pack 1, and patch Q323308.*

NOTE: *You need to reboot the AP after enabling or disabling SSL for the changes to take effect.*

- **HTTPS (Secure Web Status)**: The user can access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP comes pre-installed with all required SSL files: default certificate and private key installed. Use the drop-down menu to enable/disable this feature.
- **SSL Certificate Passphrase**: After enabling SSL, the only configurable parameter is the SSL passphrase. The default SSL passphrase is **proxim**.

  The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate.

  If you decide to upload a new certificate and private key (using TFTP or HTTP File Transfer), you need to change the SSL Certificate Passphrase for the new SSL files.

Accessing the AP through the HTTPS interface

The user should use a SSL intelligent browser to access the AP through the HTTPS interface. After configuring SSL, access the AP using **https://** followed by the AP's management IP address.

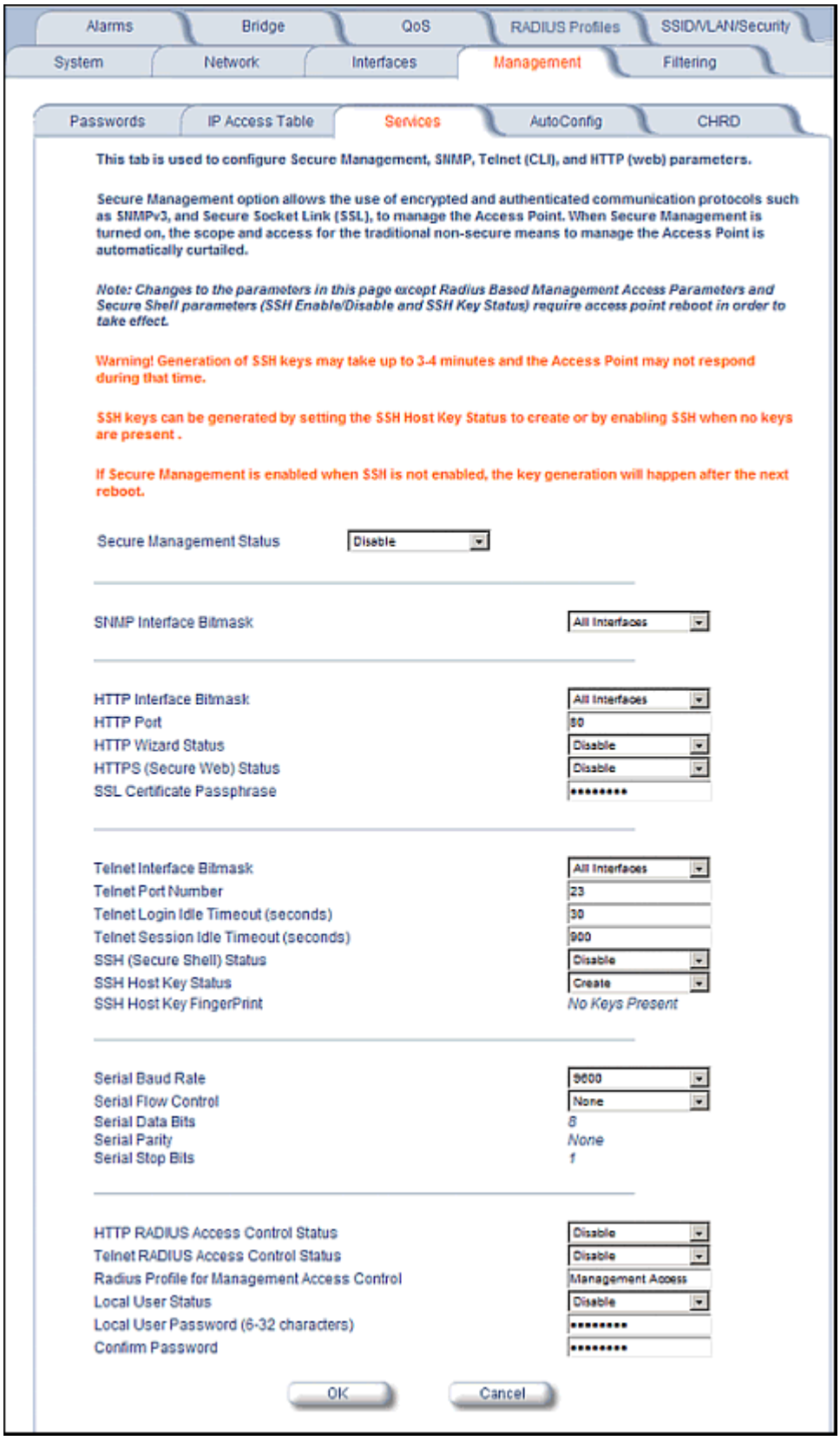


Figure 4-19 Management Services Configuration Screen

Telnet Configuration Settings

- **Telnet Interface Bitmask:** Select the interface (**Ethernet**, **Wireless-Slot A, Wireless-Slot B**, **All Interfaces**) from which you can manage the AP via telnet. This parameter can also be used to **Disable** telnet management.
- **Telnet Port Number:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select). You must reboot the Access Point if you change the Telnet Port.
- **Telnet Login Idle Timeout (seconds):** Enter the number of seconds the system will wait for a login attempt. The AP terminates the session when it times out. The range is 30 to 300 seconds; the default is 60 seconds.
- **Telnet Session Idle Timeout (seconds):** Enter the number of seconds the system will wait during a session while there is no activity. The AP will terminate the session on timeout. The range is 60 to 36000 seconds; the default is 900 seconds.

Secure Shell (SSH) Settings

The AP supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data.

The SSH server (AP) has ***host keys*** - a pair of asymmetric keys - a ***private key*** that resides on the AP and a ***public key*** that is distributed to clients that need to connect to the AP. As the client has knowledge of the server host keys, the client can verify that it is communicating with the correct SSH server. The client authentication is performed as follows:

- Using a username/password pair if RADIUS Based Management is enabled; otherwise, using a password to authenticate the user over a secure channel created using SSH.

SSH Session Setup

An SSH session is setup through the following process:

- The SSH server public key is transferred to the client using out-of-band or in-band mechanisms.
- The SSH client verifies the correctness of the server using the server's public key.
- The user/client authenticates to the server.
- An encrypted data session starts. The maximum number of SSH sessions is limited to two. If there is no activity for a specified amount of time (the Telnet Session Timeout parameter), the AP will timeout the connection.

SSH Clients

The following SSH clients have been verified to interoperate with the AP's server. The following table lists the clients, version number, and the website of the client.

Clients	Version	Website
OpenSSH	V3.4-2	http://www.openssh.com
Putty	Rel 0.53b	http://www.chiark.greenend.org.uk
Zoc	5.00	http://www.emtec.com
Axessh	V2.5	http://www.labf.com

For key generation, OpenSSH client has been verified.

Configuring SSH

Perform the following procedure to set the SSH host key and enable or disable SSH:

1. Click **Configure** > **Management** > **Services**
2. Select the **SSH Host Key Status** from the drop down menu.

   NOTE: *SSH Host Key Status can not be changed if SSH status or Secure Management is enabled.*

3. To enable/disable SSH, select Enable/Disable from the **SSH (Secure Shell) Status** drop-down menu.

NOTE: *When Secure Management is enabled on the AP, SSH will be enabled by default and cannot be disabled.*

Host keys must either be generated externally and uploaded to the AP (see Uploading Externally Generated Host Keys), generated manually, or auto-generated at the time of SSH initialization if SSH is enabled and no host keys are present. There is no key present in an AP that is in a factory default state.

To manually generate or delete host keys on the AP:

CAUTION: *SSH Host key creation may take 3 to 4 minutes during which time the AP may not respond.*

- Select **Create** to generate a new pair of host keys.
- Select **Delete** to remove the host keys from the AP. If no host keys are present, the AP will not allows connections using SSH. When host keys are created or deleted, the AP updates the fingerprint information displayed on the **Management** > **Services** page.

Uploading Externally Generated Host Keys

Perform the following procedure to upload externally generated host keys to the AP. You must upload both the SSH public key and SSH private key for SSH to work.

1. Verify that the host keys have been externally generated. The OpenSSH client has been verified to interoperate with AP's SSH server.
2. Click **Commands > Update AP > via HTTP** (or via TFTP).

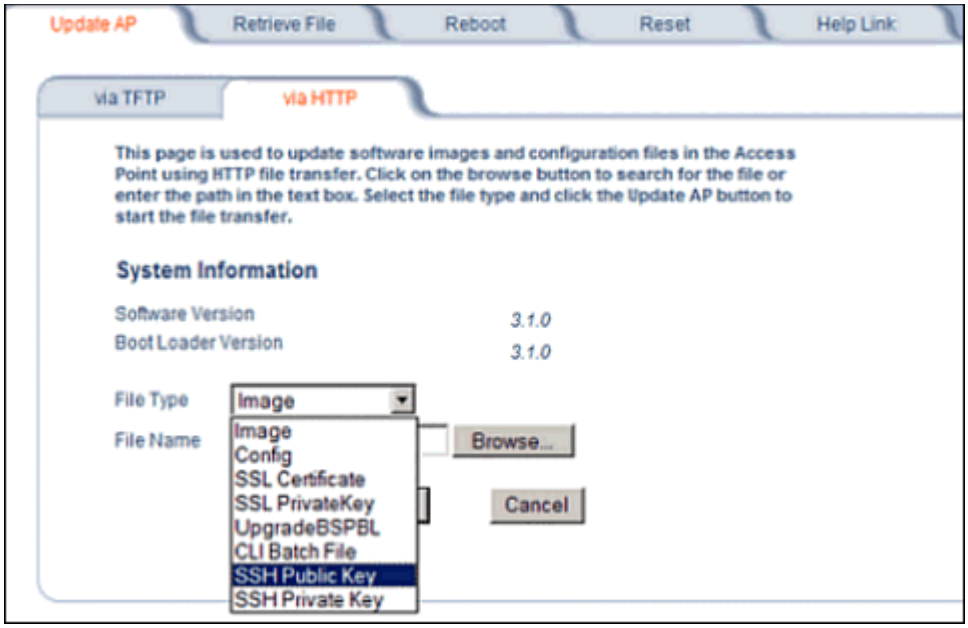


Figure 4-20 Uploading an Externally Generated SSH Public Key and SSH Private Key

3. Select **SSH Public Key** from the File Type drop-down menu.
4. Click **Browse**, select the SSH Public Key file on your local machine.
5. Click **Open**.
6. to initiate the file transfer, click the **Update AP** button.
7. Select **SSH Private Key** from the File Type drop-down menu.
8. Click **Browse**, select the SSH Private Key on your local machine.
9. Click **Open**.
10. To initiate the file transfer, click the **Update AP** button.

The fingerprint of the new SSH public key will be displayed in the **Management** > **Services** page.

Serial Configuration Settings

The serial port interface on the AP is enabled at all times. See Setting IP Address using Serial Port for information on how to access the CLI interface via the serial port. You can configure and view the following parameters:

- **Serial Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Serial Flow Control:** Select either **None** (default) or **Xon/Xoff** (software controlled) data flow control.

  NOTE: *To avoid potential problems when communicating with the AP through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).*
- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

NOTE: *The serial port bit configuration is commonly referred to as* **8N1***.*

RADIUS Based Management Access

User management of APs can be centralized by using a RADIUS server to store user credentials. The AP cross-checks credentials using RADIUS protocol and the RADIUS server accepts or rejects the user.

HTTP/HTTPS and Telnet/SSH users can be managed with RADIUS. Serial CLI and SNMP cannot be managed by RADIUS. Two types of users can be supported using centralized RADIUS management:

- **Super User**: The super user has access to all functionality of a management interface. A super user is configured in the RADIUS server by setting the filter ID attribute (returned in the RADIUS Accept packet) for the user to a value of “super user” (not case sensitive). A user is considered a super user if the value of the **filter-id** attribute returned in the RADIUS Accept packet for the user is “super user” (not case sensitive).
- **Limited User**: A limited user has access to only a limited set of functionality on a management interface. All users who are not super users are considered limited users. However, a limited user is configured in the RADIUS server by setting the **filter-id** attribute (returned in the RADIUS Accept packet) to “limited user” (not case sensitive). Limited users do not have access to the following configuration capabilities:
  - Update/retrieve files to and from APs
  - Reset the AP to factory defaults
  - Reboot the AP
  - Change management properties related to RADIUS, management modes, and management passwords.

NOTE: *When a user has both “limited user” and “super user” filter-ids configured in the Radius server, the user has limited user privileges.*

When RADIUS Based Management is enabled, a **local user** can be configured to provide Telnet, SSH, and HTTP(S) access to the AP when RADIUS servers fail. The local user has super user capabilities. When secure management is enabled, the local user can only login using secure means (i.e., SSH or SSL). When the local user option is disabled the only access to the AP when RADIUS servers are down will be through serial CLI or SNMP.

The Radius Based Management Access parameters allows you to enable HTTP or Telnet Radius Management Access, to configure a RADIUS Profile for management access control, and to enable or disable local user access, and configure the local user password. You can configure and view the following parameters:

- **HTTP RADIUS Access Control Status**: Enable RADIUS management of HTTP/HTTPS users.
- **Telnet RADIUS Access Control Status**: Enable RADIUS management of Telnet/SSH users.

- **RADIUS Profile for Management Access Control**: Specifies the RADIUS Profile to be used for RADIUS Based Management Access.
- **Local User Status**: Enables or disables the local user when RADIUS Based Management is enabled. The default local user ID is root.
- **Local User Password** and **Confirm Password**: The default local user password is public. “Root” cannot be configured as a valid user for Radius based management access when local user access is enabled.

Automatic Configuration (AutoConfig)

The Automatic Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Automatic Configuration is disabled by default. The configuration process for Automatic Configuration varies depending on whether the AP is configured for dynamic or static IP.

When an AP is configured for dynamic IP, the Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. When configured for static IP, these parameters are instead configured in the AP interface.

After setting up automatic configuration you must reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If Syslog is configured, a Syslog message will appear indicating the success or failure of the Automatic Configuration.

Auto Configuration and the CLI Batch File

The Auto Configuration feature allows download of the LTV (Length, Type, Value) format configuration file or the CLI Batch file. The LTV file contains parameters used by the AP; the CLI Batch file contains CLI executable commands used to set AP parameters. The AP detects whether the uploaded file is LTV format or a CLI Batch file. If the AP detects an LTV file, it stores the file in the AP’s flash memory. If the AP detects a CLI Batch file (a file with an extension of .cli), the AP executes the commands contained in the file immediately. The AP will reboot after executing the CLI Batch file. Auto Configuration will not result in repeated reboots if the CLI Batch file contains rebootable parameters.

For more information, see the CLI Batch File section.

Set up Automatic Configuration for Static IP

Perform the following procedure to enable and set up Automatic Configuration when you have a static IP address for the TFTP server.

1. Click **Configure** > **Management** > **AutoConfig**.
   The Automatic Configuration Screen appears.
2. Check **Enable Auto Configuration**.
3. Enter the **Configuration Filename**.
4. Enter the IP address of the TFTP server in the **TFTP Server Address** field.

   NOTE: *The default filename is “config”. The default TFTP IP address is “169.254.128.133” for AP-4000/4000M/4900M.*

5. Click **OK** to save the changes.
6. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:
   - AutoConfig for Static IP
   - TFTP server address and configuration filename
   - AutoConfig Successful

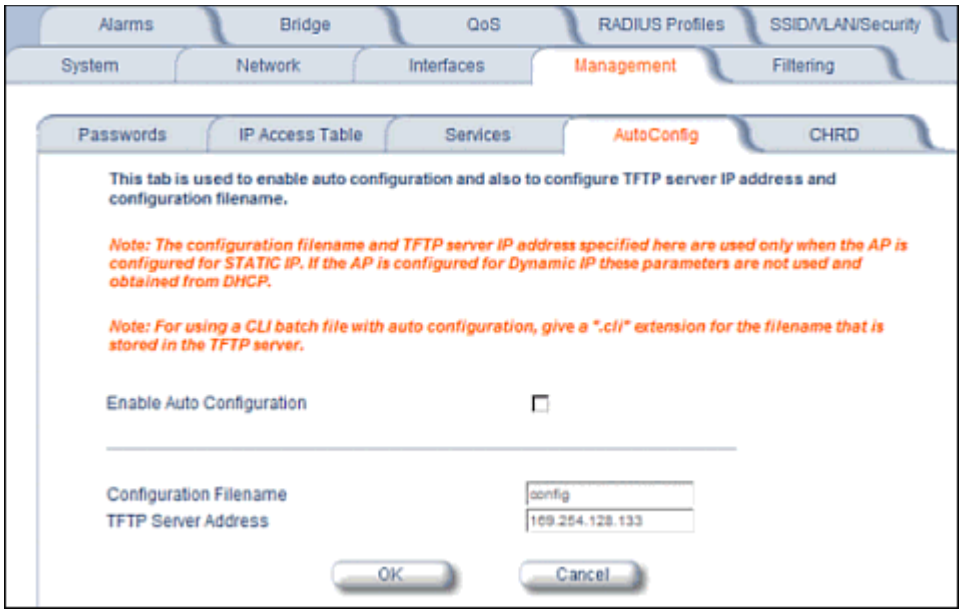


Figure 4-21 Automatic Configuration Screen

Set up Automatic Configuration for Dynamic IP

Perform the following procedure to enable and set up Automatic Configuration when you have a dynamic IP address for the TFTP server via DHCP.

The Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. A Syslog server address is also contained in the DHCP response, allowing the AP to send Auto Configuration success and failure messages to a Syslog server.

NOTE: *The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP.*

1. Click **Configure** > **Management** > **AutoConfig**.
   The Automatic Configuration Screen appears.
2. Check **Enable Auto Configuration**.

   When the AP is Configured with Dynamic IP, the DHCP server should be configured with the TFTP Server IP address ("Boot Server Host Name", option 66) and Configuration file ("Bootfile name", option 67) as follows (note that this example uses a Windows 2000 server):
3. **Select DHCP Server** > **DHCP Option** > **Scope**.
   The DHCP Options: Scope Screen appears.

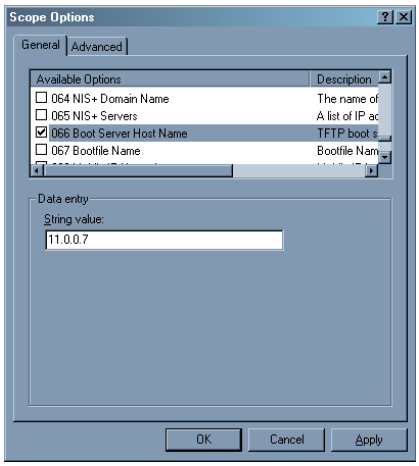


Figure 4-22 DHCP Options: Setting the Boot Server Host Name

4. Add the Boot Server Hostname and Boot Filename parameters to the Active Options list.
5. Set the value of the Boot Server Hostname Parameter to the hostname or IP Address of the TFTP server. For example: 11.0.0.7.

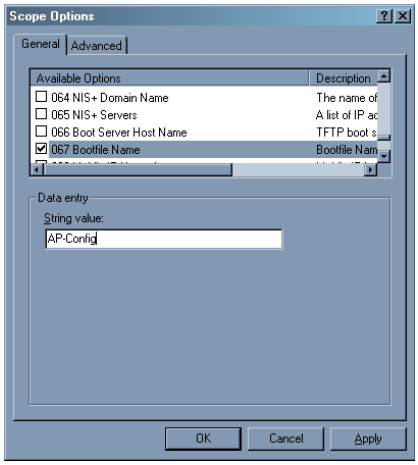


Figure 4-23 DHCP Options: Setting the Bootfile Name

6. Set the value of the Bootfile Name parameter to the Configuration filename. For example: AP-Config
7. If using Syslog, set the Log server IP address (option 7, Log Servers).
8. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:
   - AutoConfig for Dynamic IP
   - TFTP server address and configuration filename
   - AutoConfig Successful

Hardware Configuration Reset (CHRD)

Hardware Configuration Reset Status is a parameter that defines the hardware configuration reset behavior of the AP (i.e., what effect pressing the reload button has on an AP operating in normal operating mode).

If a user loses or forgets the AP's HTTP/Telnet/SNMP password, the reset button on the AP provides a way to reset the AP to default configuration values to gain access to the AP. However, in AP deployments where physical access to the

AP is not protected, an unauthorized person could reset the AP to factory defaults and thus gain control of the AP. The user can disable the hardware configuration reset functionality to prevent unauthorized access.

The hardware configuration reset feature operates as follows:

- When hardware configuration reset is enabled, the user can press the hardware reload button for 10 seconds when the AP is in normal operational mode in order to delete the AP configuration.
- When hardware configuration reset is disabled, pressing the reload button when the AP is in normal operational mode does not have any effect on the AP.
- The hardware configuration reset parameter does not have any effect on the functionality of the reload button to delete the AP image during AP boot loaded execution.
- The default hardware configuration reset status is enabled. When disabling hardware configuration reset, the user is recommended to configure a configuration reset password. A configuration reset option appears on the serial port during boot up, before the AP reads its configuration and initializes.
- Whenever the AP is reset to factory default configuration, hardware configuration reset status is enabled and the configuration reset password is set to the default, “public”.
- If secure mode is enabled in the AP, only secure (SSL, SNMPv3, SSH) users can modify the values of the Hardware Configuration Reset Status and the configuration reset password.

Configuration Reset via Serial Port During Bootup

If hardware configuration reset is disabled, the user gets prompted by a configuration reset option to reset the AP to factory defaults during boot up from the serial interface. By pressing a key sequence (ctrl-R), the user gets prompted to enter a configuration reset password before the configuration is reset.

NOTE: *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disable.*

Configuring Hardware Configuration Reset

Perform the following procedure to configure Hardware Configuration Reset and to set the Configuration Reset Password. See Figure 4-24.

1. Click **Configure** > **Management** > **CHRD**.

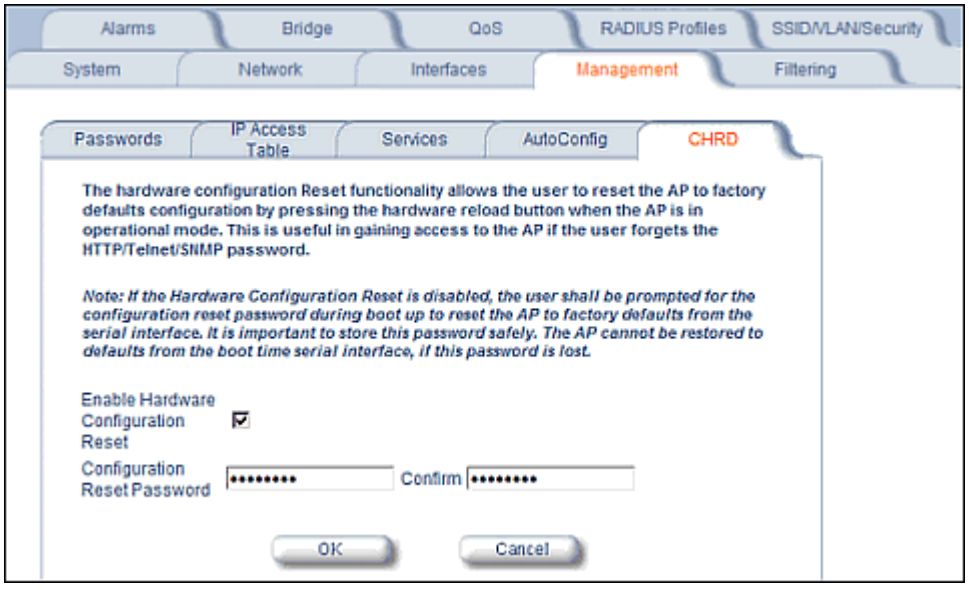


Figure 4-24 Hardware Configuration Reset

2. Check (enable) or uncheck (disable) the **Enable Hardware Configuration Reset** checkbox.
3. Change the default Configuration Reset Password in the “Configuration Reset Password” and “Confirm” fields.
4. Click OK.
5. Reboot the AP.

NOTE: *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disable.*

Procedure to Reset Configuration via the Serial Interface

1. During boot up, observe the message output on the serial interface.

   The AP prompts the user with the message: “Press ctrl-R in 3 seconds to choose configuration reset option.”
2. Enter ctrl-R within 3 seconds after being prompted.

   The AP prompts the user with “Press ctrl-Z to continue with normal boot up or enter password to reset configuration.” If the user enters ctrl-Z, the AP continues to boot with the stored configuration.
3. Enter the configuration reset password. The default configuration reset password is “public”.

   When the correct configuration reset password is entered, the AP gets reset to factory defaults and displays the message “AP has been reset to Factory Default Settings.” The AP continues to boot up. If an incorrect configuration reset password is entered, the AP shows an error message and reprompts the user. If the incorrect password is entered three times in a row, the AP proceeds to boot up.

Filtering

The Access Point's Packet Filtering features help control the amount of traffic exchanged between the wired and wireless networks. There are four sub-tabs under the Filtering heading:

- Ethernet Protocol
- Static MAC
- Advanced
- TCP/UDP Port

Ethernet Protocol

The Ethernet Protocol Filter blocks or forwards packets based on the Ethernet protocols they support.

Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interface or interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
   - **Ethernet:** Packets are examined at the Ethernet interface
   - **Wireless-Slot A or Wireless-Slot B:** Packets are examined at the Wireless A or B interfaces
   - **All Interfaces:** Packets are examined at both interfaces
   - **Disabled:** The filter is not used
2. Select the **Filter Operation Type**.
   - If set to **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table will pass through the bridge.
   - If set to **Block**, the bridge will block enabled Ethernet Protocols listed in the Filter Table.
3. Configure the **Ethernet Protocol Filter Table**. This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.
   - To add an entry, click **Add**, and then specify the **Protocol Number** and a **Protocol Name**.
     — **Protocol Number:** Enter the protocol number. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
     — **Protocol Name:** Enter related information, typically the protocol name.
   - To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.
   - An entry's status must be enabled in order for the protocol to be subject to the filter.

Static MAC

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is properly configured, the AP can block traffic between wired devices and wireless devices based on MAC address.

For example, you can set up a Static MAC filter to prevent wireless clients from communicating with a specific server on the Ethernet network. You can also use this filter to block unnecessary multicast packets from being forwarded to the wireless network.

NOTE: *The Static MAC Filter is an advanced feature. You may find it easier to control wireless traffic via other filtering options, such as Ethernet Protocol Filtering.*

Each static MAC entry contains the following fields:

- **Wired MAC Address**
- **Wired Mask**
- **Wireless MAC Address**
- **Wireless Mask**
- **Comment:** This field is optional.

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1).)

Taken together, a MAC Address/Mask pair specifies an address or a range of MAC addresses that the AP will look for when examining packets. The AP uses Boolean logic to perform an “AND” operation between the MAC Address and the Mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the Mask (where 0 is any value and F is the value specified in the MAC address). A Mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a Mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC Address.

For example, if the MAC Address is 00:20:A6:12:54:C3 and the Mask is FF:FF:FF:00:00:00, the AP will examine the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the Mask is FF:FF:FF:FF:FF:FF, the AP will only look for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want block:

- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC Address and Wired Mask (leave the Wireless MAC Address and Wireless Mask set to all zeros).
- To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC address and Wireless Mask (leave the Wired MAC Address and Wired Mask set to all zeros).
- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

A maximum of 200 entries can be created in the Static MAC filter table. To create an entry, click **Add** and enter the appropriate MAC addresses and Masks to setup a filter. The entry is enabled automatically when saved. To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

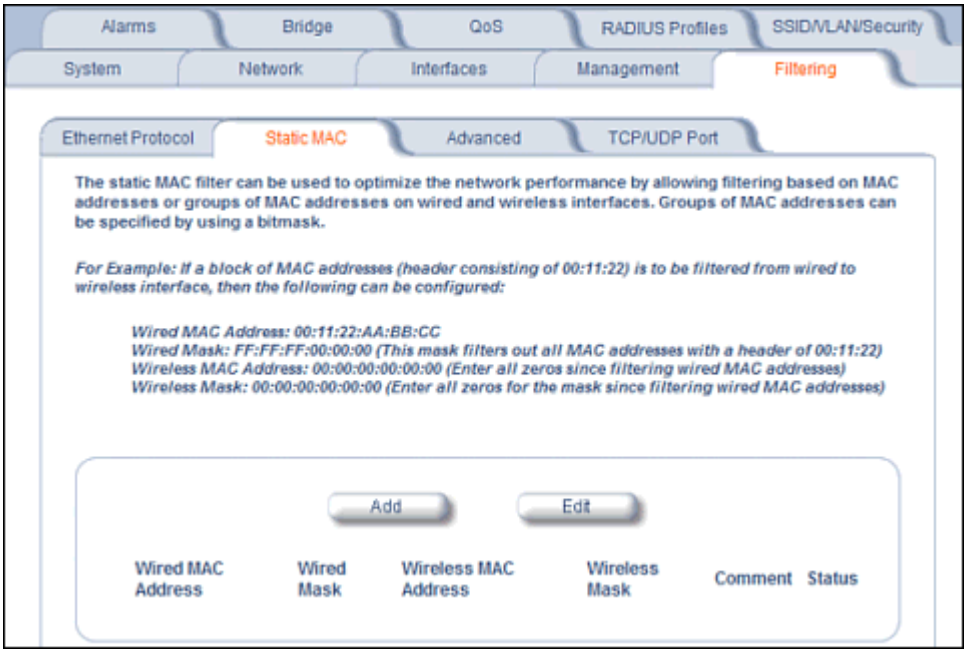


Figure 4-25 Static MAC Configuration Screen

Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC address for each unit is as follows:

- Wired Server: 00:40:F4:1C:DB:6A
- Wireless Client 1: 00:02:2D:51:94:E4

- Wireless Client 2: 00:02:2D:51:32:12
- Wireless Client 3: 00:20:A6:12:4E:38

Prevent Two Specific Devices from Communicating

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 can still communicate with the Wired Server.

Prevent Multiple Wireless Devices from Communicating with a Single Wired Device

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical “AND” is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

Prevent All Wireless Devices from Communicating with a Single Wired Device

Configure the following settings to prevent all three Wireless Clients from communicating with Wired Server 1:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point blocks all traffic between Wired Server 1 and all wireless clients.

Prevent a Wireless Device from Communicating with the Wired Network

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet:

- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The Access Point blocks all traffic between Wireless Client 3 and the Ethernet network.

Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN

If there are devices on your Ethernet network that use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

Advanced

You can configure the following advanced filtering options:

- **Enable Proxy ARP:** Place a check mark in the box provided to allow the Access Point to respond to Address Resolution Protocol (ARP) requests for wireless clients. When enabled, the AP answers ARP requests for wireless stations without actually forwarding them to the wireless network. If disabled, the Access Point will bridge ARP requests for wireless clients to the wireless LAN.
- **Enable IP/ARP Filtering:** Place a check mark in the box provided to allow IP/ARP filtering based on the IP/ARP Filtering Address and IP Mask. Leave the box unchecked to prevent filtering. If enabled, you should also configure the IP/ARP Filtering Address and IP/ARP IP Mask.
  - **IP/ARP Filtering Address:** Enter the Network filtering IP Address.
  - **IP/ARP IP Mask:** Enter the Network Mask IP Address.

The following protocols are listed in the Advanced Filter Table:

- **Deny IPX RIP**
- **Deny IPX SAP**
- **Deny IPX LSP**
- **Deny IP Broadcasts**
- **Deny IP Multicasts**

The AP can filter these protocols in the wireless-to-Ethernet direction, the Ethernet-to-wireless direction, or in both directions. Click **Edit** and use the **Status** field to Enable or Disable the filter.

TCP/UDP Port

Port-based filtering enables you to control wireless user access to network services by selectively blocking TCP/UDP protocols through the AP. A user specifies a Protocol Name, Port Number, Port Type (TCP, UDP, or TCP/UDP), and filtering interfaces (Wireless only, Ethernet only, all interfaces, or no interfaces) in order to block access to services, such as Telnet and FTP, and traffic, such as NETBIOS and HTTP.

For example, an AP with the following configuration would discard frames received on its Ethernet interface with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets.

Protocol Type (TCP/UDP)	Destination Port Number	Protocol Name	Interface	Status (Enable/Disable)
UDP	137	NETBIOS Name Service	Ethernet	Enable

Adding TCP/UDP Port Filters

1. Place a check mark in the box labeled **Enable TCP/UDP Port Filtering**.
2. Click **Add** under the ***TCP/UDP Port Filter Table*** heading.
3. In the ***TCP/UDP Port Filter Table***, enter the Protocol Names to filter.

4. Set the destination Port Number (a value between 1 and 65535) to filter. See the IANA Web site at http://www.iana.org/assignments/port-numbers for a list of assigned port numbers and their descriptions.
5. Set the Port Type for the protocol: **TCP**, **UDP**, or both (**TCP/UDP**).
6. Set the **Interface** to filter:
   - Ethernet
   - Wireless Slot A
   - Ethernet and Wireless Slot A
   - Wireless Slot B
   - Ethernet and Wireless Slot B
   - Wireless Slot A and B
   - All interfaces
7. Click **OK**.

Editing TCP/UDP Port Filters

1. Click **Edit** under the ***TCP/UDP Port Filter Table*** heading.
2. Make any changes to the Protocol Name or Port Number for a specific entry, if necessary.
3. In the row that defines the port, set the **Status** to **Enable**, **Disable**, or **Delete**, as appropriate.
4. Select **OK**.

Alarms

The Alarms tab has the following sub-tabs:

- Groups
- Alarm Host Table
- Syslog
- Rogue Scan

Groups

Alarm groups can be enabled or disabled via the Web interface. Place a check mark in the box provided to enable a specific group. Remove the check mark from the box to disable the alarms. Alarm severity levels are as follows:

- **Critical alarms** will often result in severe disruption in network activity or an automatic reboot of the AP.
- **Major alarms** are usually activated due to a breach in the security of the system. Clients cannot be authenticated because an attempt at unauthorized access into the AP has been detected.
- **Informational alarms** provide the network administrator with some general information about the activities the AP is performing.

Configuration Trap Group

Trap Name	Description	Severity Level
oriTrapDNSIPNotConfigured	DNS IP address not configured	Major
oriTrapRADIUSAuthenticationNotConfigured	RADIUS Authentication not configured	Major
oriTrapRADIUSAccountingNotConfigured	RADIUS Accounting not configured	Major
oriTrapDuplicateIPAddressEncountered	Another network device with the same IP address exists	Major
oriTrapDHCPRelayServerTableNotConfigured	The DHCP relay agent server table is empty or not configured	Major
oriTrapVLANIDInvalidConfiguration	A VLAN ID configuration is invalid	Major
oriTrapAutoConfigFailure	Auto configuration failed	Minor
oriTrapBatchExecFailure	The CLI Batch execution fails for the following reasons: • Illegal Command is parsed in the CLI Batch file • Execution error is encountered while executing CLI Batch file • Bigger file size than 100 Kbytes	Minor
oriTrapBatchFileExecStart	The CLI Batch execution begins after file is uploaded	Minor
oriTrapBatchFileExecEnd	The execution of CLI Batch file ends.	Minor

Security Trap Group

Trap Name	Description	Severity Level
oriTrapInvalidEncryptionKey	Invalid encryption key has been detected.	Critical
oriTrapAuthenticationFailure	Client authentication failure has occurred. Authentication failures can range from: • MAC Access Control table • RADIUS MAC authentication • 802.1x authentication specifying the EAP-Type • WORP mutual authentication • SSID authorization failure specifying the SSID • VLAN ID authorization failure specifying the VLAN ID	Major
oriTrapUnauthorizedManagerDetected	Unauthorized manager has attempted to view and/or modify parameters	Major
oriTrapRADScanComplete	RAD scan is successfully completed	Informational
oriTrapRADScanResults	Provides information on the RAD Scan results	Informational
oriTrapRogueScanStationDetected	Rogue station detected	Informational
oriTrapRogueScanCycleComplete	Rogue scan successfully completed	Informational

Wireless Interface/Card Trap Group

Trap Name	Description	Severity Level
oriTrapWLCFailure	General failure wireless interface/card failure.	Critical
oriTrapWLCRadarInterferenceDetected	Radar interference detected on the channel being used by the wireless interface	Major
MIC Attack Detected	Supported in Web interface only	Major
MIC Attack Report Detected	Supported in Web interface only	Major

Operational Trap Group

Trap Name	Description	Severity Level
oriTrapUnrecoverableSoftwareErrorDetected	Unrecoverable software error detected. Causes software watch dog timer to expire, which in turn causes the device to reboot.	Critical
oriTrapRADIUSServerNotResponding	RADIUS server not responding to authentication requests sent from the RADIUS client in the device	Major
oriTrapModuleNotInitialized	Module (hardware or software) not initialized	Major
oriTrapDeviceRebooting	Device rebooting	Informational
oriTrapTaskSuspended	Task suspended	Critical
oriTrapBootPFailed	Response to the BootP request not received; device not dynamically assigned an IP address	Major

Trap Name	Description	Severity Level
oriTrapDHCPFailed	Response to the DHCP client request not received; device not dynamically assigned an IP address	Major
oriTrapDNSClientLookupFailure	DNS client attempts to resolve a specified hostname (DNS lookup) and a failure occurs because either the DNS server is unreachable or there is an error for the hostname lookup. Trap specifies the hostname that was being resolved.	Major
oriTrapSSLInitializationFailure	SSL initialization failure	Major
oriTrapWirelessServiceShutdown	Wireless interface has shutdown services for wireless clients	Informational
oriTrapWirelessServiceResumed	Wireless interface has resumed service and is ready for wireless client connections	Informational
oriTrapSSHInitializationStatus	SSH initialization status	Major
oriTrapVLANIDUserAssignment	User is assigned a VLAN ID from the RADIUS server	Informational
oriTrapDHCPLeaseRenewal	AP requests DHCP renewal and receives new information from the DHCP server. Information includes the DHCP server IP address that replied to the DHCP client request, and the IP address, subnet mask, and gateway IP address returned from the DHCP server.	Informational

Flash Memory Trap Group

Trap Name	Description	Severity Level
oriTrapFlashMemoryEmpty	No data present in flash memory	Informational
Flash Memory Corrupted	Flash memory corrupted	Critical
oriTrapFlashMemoryRestoringLastKnownGoodConfiguration	Current/original configuration data file is found to be corrupted, and the device loads the last known good configuration file	Informational

TFTP Trap Group

Trap Name	Description	Severity Level
oriTrapTFTPFailedOperation	TFTP operation failed	Major
oriTrapTFTPOperationInitiated	TFTP operation Initiated	Informational
oriTrapTFTPOperationCompleted	TFTP operation completed	Informational

Image Trap Group

Trap Name	Description	Severity Level
oriTrapZeroSizeImage	Zero size image loaded onto device	Major
oriTrapInvalidImage	Invalid image loaded onto device	Major
oriTrapImageTooLarge	Image loaded on the device exceeds the size limitation of flash	Major
oriTrapIncompatibleImage	Incompatible image loaded onto device	Major
oriTrapInvalidImageDigitalSignature	Image with invalid digital signature is loaded onto device	Major

SNTP Trap Group

Trap Name	Description	Severity Level
oriTrapSNTPFailure	SNTP time retrieval failure	Minor
oriTrapSNTPFailure	SNTP sync-up failure	Minor

Generic Trap Group

Trap Name	Description	Severity Level
oriTrapGenericNotification (see following table)	Generic SNMP Trap	Variable

A generic SNMP trap may be sent for any of the following reasons:

Trap Reason/Type	Additional Trap Information	Severity Level
Mesh Connection Failure	Connection failure reason	Major
Link Integrity Failure	Target IP address of down link	Major
Topology Change	Ethernet MAC address of Mesh AP causing change; Mesh SSID	Informational

System Feature/License Group

Trap Name	Description	Severity Level
oriTrapIncompatibleLicenseFile	Incompatible license file	Major
oriTrapInvalidLicenseFile	Invalid license file	Major

In addition, the AP supports these standard traps, which are always enabled:

RFC 1215-Trap

Trap Name	Description	Severity Level
coldStart	AP is on or rebooted	Informational
linkUp	AP's Ethernet interface link is up (working)	Informational
linkDown	AP's Ethernet interface link is down (not working)	Informational

Bridge MIB (RFC 1493) Alarms

Trap Name	Description	Severity Level
New Root	AP has become the new root in the Spanning Tree network	Informational
topologyChange	Trap is not sent if a newRoot trap is sent for the same transition	Informational

All these alarm groups correspond to System Alarms that are displayed in the System Status Screen, including the traps that are sent by the AP to the SNMP managers specified in the Alarm Host Table.

Alarm Host Table

To add an entry and enable the AP to send SNMP trap messages to a Trap Host, click **Add**, and then specify the IP Address and Password for the Trap Host.

NOTE: *Up to 10 entries are possible in the Alarm Host table.*

- **IP Address:** Enter the Trap Host IP Address.
- **Password:** Enter the password in the **Password** field and the **Confirm** field.
- **Comment:** Enter an optional comment, such as the alarm (trap) host station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

Syslog

The Syslog messaging system enables the AP to transmit event messages to a central server for monitoring and troubleshooting. The access point logs “Session Start (Log-in)” and “Session Stop (Log-out)” events for each wireless client as an alternative to RADIUS accounting.

See RFC 3164 at http://www.rfc-editor.org for more information on the Syslog standard.

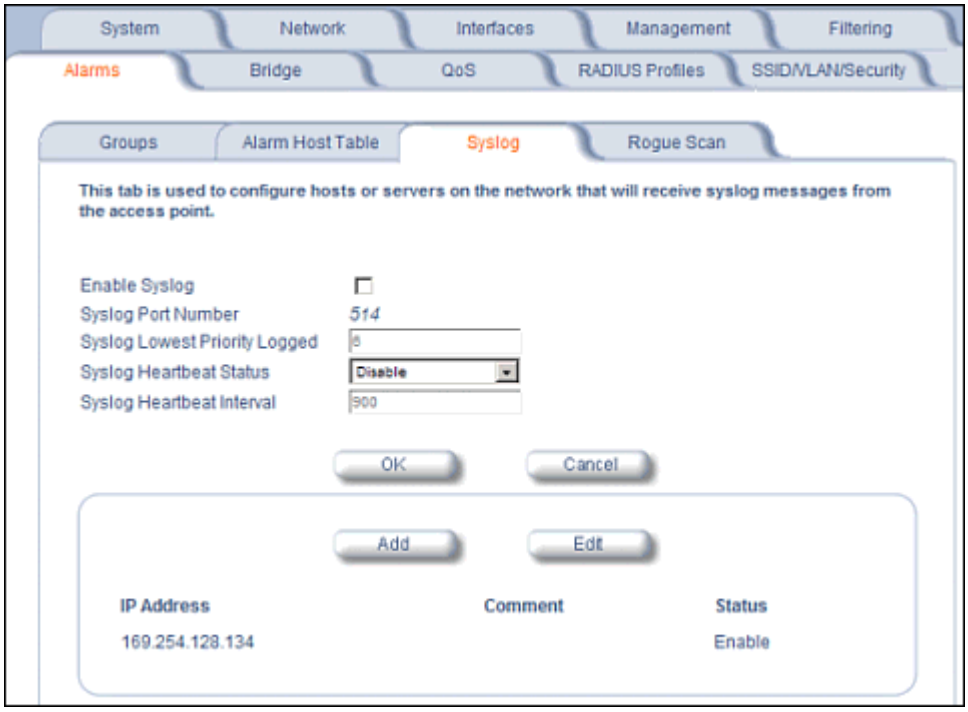


Figure 4-26 Syslog Configuration Screen

Setting Syslog Event Notifications

Syslog Events are logged according to the level of detail specified by the administrator. Logging only urgent system messages will create a far smaller, more easily read log than a log of every event the system encounters. Determine which events to log by selecting a priority defined by the following scale:

Event	Priority	Description
LOG_EMERG	0	System is unusable
LOG_ALERT	1	Action must be taken immediately
LOG_CRIT	2	Critical conditions
LOG_ERR	3	Error conditions
LOG_WARNING	4	Warning conditions
LOG_NOTICE	5	Normal but significant condition
LOG_INFO	6	Informational
LOG_DEBUG	7	Debug-level messages

Configuring Syslog Event Notifications

You can configure the following Syslog settings from the HTTP interface:

- **Enable Syslog:** Place a check mark in the box provided to enable system logging.
- **Syslog Port Number:** This field is read-only and displays the port number (514) assigned for system logging.

- **Syslog Lowest Priority Logged:** The AP will send event messages to the Syslog server that correspond to the selected priority number and any priority numbers below it. For example, if set to 6, the AP will transmit event messages labeled priority 0 to 6 to the Syslog server. This parameter supports a range between 0 and 7; 6 is the default.
- **Syslog Heartbeat Status:** When Heartbeat is enabled, the AP periodically sends a message to the Syslog server to indicate that it is active.
- **Syslog Heartbeat Interval:** If Syslog Heartbeat Status is enabled this field provides the interval for the heartbeat in seconds (between 1 and 604800). The default is 900 seconds.
- **Syslog Host Table:** This table specifies the IP addresses of a network servers that the AP will send Syslog messages to. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  - **IP Address:** Enter the IP Address for the management host.
  - **Comment:** Enter an optional comment such as the host name.
  - **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field's value.

Syslog Messages

The following messages are supported in the AP:

Syslog Message Name	Priority	Severity	Description
Auto Configuration using DHCP	6	Informational	Configuration filename and TFTP server address are obtained from DHCP when dynamic IP is configured on the device.
Auto Configuration using Static IP	6	Informational	Configured TFTP server address and configuration filename is used when Static IP is configured on the device.
TFTP Server IP and configuration filename not present in DHCP response	4	Minor	Configuration filename and/or TFTP server address is not present in the DHCP response when using DHCP.
TFTP Server IP Address used in AutoConfig feature	6	Informational	TFTP server IP address used for AutoConfig.
TFTP Server filename used in AutoConfig feature	6	Informational	TFTP filename used for AutoConfig.
Auto Configuration TFTP Download Failure	4	Minor	TFTP download of a configuration file for AutoConfig fails for the following reasons: Incorrect or non-reachable TFTP server address Incorrect or unavailable configuration filename TFTP transfer timeout.
Image Compatibility Check, Invalid Image	2	Major	One of the following failures occurs: Invalid Signature Zero File Size Large File Non VxWork Image Incompatible Image
AP Heartbeat Status	5	Informational	AP syslog keep alive message.

Syslog Message Name	Priority	Severity	Description
Client Login Authentication Status	6	Informational	Client logs in/authenticates. Message includes: • Client MAC Address • Authentication Type = None, ACL, RADIUS MAC, 802.1X • Cipher Type = None, WEP, TKIP, AES • Status = Allow, Deny • SSID to which client is connecting Sample Message: <client mac address> | Status = <value> | SSID = <value> | Auth Type = <value> | Cipher Type = <value>
Client De-Authentication Status	6	Informational	Client de-authenticates. Message includes: • Client MAC Address • Cipher Type = None, WEP, TKIP, AES • Status = De-authentication reason, which can be any of the following: – Unknown reason – Stale authentication information – Authenticated STA leaving BSS – Inactivity – Association error – Class 2 frame received from non-authenticated STA – Class 3 frame received from non-associated STA – Associated STA leaving BSS – STA requesting information, but not yet authenticated – Enhanced security (RSN) required – Enhanced security (RSN) used inconsistently – Invalid Information Element – MIC Failure – WPA module de-auth • SSID to which client was connected Sample Message: <client mac address> | Status = <value> | SSID = <value> | Cipher Type = <value>
RADIUS Accounting Start and Stop Messages	6	Informational	Start and Stop accounting messages for wireless clients.
CLI Configuration File Start Execution	6	Informational	CLI configuration file execution starts.
CLI Configuration File End Execution	6	Informational	CLI configuration file execution ends.

Syslog Message Name	Priority	Severity	Description
CLI Configuration File Execution Errors	4	Minor	There is an error in execution of the CLI configuration file. The message specifies the filename, line number, and error reason.
SSH Initialization Failure	3	Major	One of the following failures occurs: Keys not present Keys cannot be generated Internal error (no available resources)
SSH Key Generation Successful	6	Informational	SSH Key generation is successful.
Wireless Service Shutdown	6	Informational	Wireless service is shutdown.
Wireless Service Resume	6	Informational	Wireless service resumes.
First MIC Report Attack	4	Minor	First MIC report attack is detected.
Second MIC Report Attack	4	Minor	Second MIC report attack is detected.
MIC Attack from Wireless Station	4	Minor	A MIC attack is detected from a wireless station.
SNTP Time Retrieval Failure	4	Minor	SNTP Client in the AP fails to retrieve time information from the configured SNTP servers. Also included in message: IP Address of SNTP server.
SNTP Time Sync-Up Failure	4	Minor	SNTP Client in the AP fails to synchronize the time with the SNTP server it was communicating with. Also included in message: IP Address of SNTP server.
Incompatible license file	3	Major	Incompatible license file is stored in flash memory during initialization or license file download. Also included in message: incompatibility reason.
Invalid license file	3	Major	Invalid license file is stored in flash memory during initialization or license file download. The license file is found to be invalid if the signed checksum verification fails.
Mesh Connection Failure	3	Major	AP fails to connect with an uplink Mesh AP or Mesh portal. Also included in message: uplink Mesh portal/AP MAC address, Mesh SSID, and reason for connection failure.
Link Integrity Failure	3	Major	Link integrity feature determines that link integrity target is down. Also included in message: Link Integrity target IP address.
Topology Change	6	Informational	Mesh AP changes its uplink mesh connection. Also included in message: uplink Mesh AP/portal MAC address and Mesh SSID.

Rogue Scan

The Rogue Scan feature provides an additional security level for wireless LAN deployments. Rogue Scan uses the selected wireless interface(s) for scanning its coverage area for Access Points and clients.

A centralized *Network Manager* receives MAC address information from the AP on all wireless clients detected by the AP. The Network Manager then queries all wired switches to find out the inbound switch/port of these wireless clients. If the switch/port does not have a valid Access Point connected to it as per a pre-configured database, the Network Manager proceeds to block that switch/port and prevent the Rogue AP from connecting to the wired network.

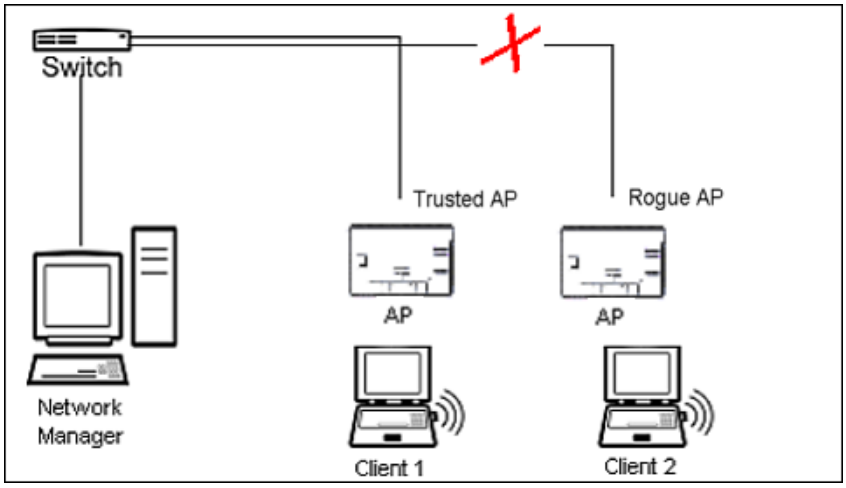


Figure 4-27 Preventing Rogue AP Attacks

The figure above shows Client 1 connected to a Trusted AP and Client 2 connected to a Rogue AP. The Trusted AP scans the networks, detects Client 2, and notifies the Network Manager. The Network Manager uses SNMP/CLI to query the wired switch to find the inbound switch port of Client 2's packets. The Network Manager verifies that this switch/router and port does not have a valid Access Point as per the administrator's database. Thus it labels Client 2's AP as a Rogue AP and proceeds to prevent the Rogue AP attack by blocking this switch's port.

Multi-Band Scanning

Rogue Scan detects Rogue stations in all bands (i.e., 2.4 GHz and 5 GHz for interfaces that support 802.11a/g multi-band operation. During Rogue Scan the AP scans every channel in its configured regulatory domain; the AP scans both the 2.4 GHz and 5 GHz bands for wireless interfaces supporting 802.11a/g multi-band operation.

APs can be detected either by active scanning using 802.11 probe request frames or passively by detecting periodic beacons, or both. Wireless clients are detected by monitoring 802.11 connection establishment messages such as association/authentication messages or data traffic to or from the wireless clients.

There are two scanning modes available per wireless interface: continuous scanning mode and background scanning mode.

Continuous Scanning Mode

The continuous scanning mode is a dedicated scanning mode where the wireless interface performs scanning alone and does not perform the normal AP operation of servicing client traffic.

In continuous scanning mode the AP scans each channel for a channel scan time of one second and then moves to the next channel in the scan channel list. With a channel scan time of one second, the scan cycle time will take less than a minute (one second per channel). Once the entire scan channel list has been scanned the AP restarts scanning from the beginning of the scan channel list.

Background Scanning Mode

In background scanning mode the AP performs background scanning while performing normal AP operations on the wireless interface.

You can configure the **scan cycle time** between 1-1440 minutes (24 hours). The scan cycle time indicates how frequently a channel is sampled and defines the minimum attack period that can go unnoticed.

In background scanning mode the AP will scan one channel then wait for a time known as channel scan time. The channel scan time affects the amount of data collected during scanning and defines the maximum number of samples (possible detections) in one scan. This is increased to improve scanning efficiency; the tradeoff is that it decreases

throughput. The optimum value for this parameter during background scanning mode is 20ms.The channel scan time is calculated from the scan cycle time parameter and the number of channels in the scan channel list as follows:

intra-channel scan time = (scan cycle time - (channel scan time * number of channels in the scan list))/number of channels in the scan list.

NOTE: *If the AP is configured as a Mesh AP, the background scanning interval will be the same as the Mesh scanning interval (20 ms if there is no uplink, or 180 ms if there is an uplink).*

Rogue Scan Data Collection

The AP stores information gathered about detected stations during scanning in a Rogue Scan result table. The Rogue Scan result table can store a maximum of 2000 entries. When the table fills, the oldest entry gets overwritten. The Rogue Scan result table lists the following information about each detected station:

- Station Type: indicates one of the following types of station:
  - Unknown station
  - AP station
  - Infrastructure Client Station
  - IBSS Client Station
- MAC Address of the detected station
- Channel: the working channel of the detected station
- SNR: the SNR value of the last frame from the station as received by the AP
- BSSID: the BSSID field stores the:
  - MAC address of the associated Access Point in the case of a client.
  - Zero MAC address or MAC address of the partner Access Point if the AP is a partner of a WDS link

The AP ages out older entries in the Rogue Scan result table if a detected station is inactive for more than the Scan Result Table Ageing Time.

Rogue Scan

Perform this procedure to enable Rogue Scan on a particular interface or interfaces and define the Scan Interval and Scan Interface. See Figure 4-28 on page 96.

The Rogue Scan screen also displays the number of new access points and clients detected in the last scan on each wireless interface.

1. Enable the Security Alarm Group. Select the Security Alarm Group link from the Rogue Scan screen. Configure a Trap Host to receive the list of access points (and clients) detected during the scan.
2. Click **Configure** > **Alarms** > **Rogue Scan**.
3. Enable Rogue Scan on a wireless interface by checking **Enable Rogue Scan.**

NOTE: *Rogue Scan cannot be enabled on a wireless interface when the Wireless Service Status on that interface is shutdown. First, resume service on the wireless interface.*

4. Enter the **Scan Mode**. Select Background Scanning or Continuous Scanning. In Continuous Scanning mode the AP stops normal operation and scans continuously on that interface. In Background Scanning mode, the AP performs background scanning while doing normal AP operation on that interface.
5. If the Scan Mode is Background Scanning, then enter the **Scan Interval**.
   - The Scan Interval specifies the time period in minutes between scans in Background Scanning mode and can be set to any value between 1 and 1440 minutes.
6. Configure the **Scan Result Table Ageing Time**. The AP ages out older entries in the Rogue Scan result table if a detected station is inactive for more than this time. The valid range is from 60-7200 minutes, the default is 60 minutes.

7. Configure the **Scan Results Trap Notification Mode** to control the notification behavior when APs or stations are detected in a scan:
   - No Notification
   - Notify AP
   - Notify Client
   - Notify All (Notify both AP and Client detection)
8. Configure the **Scan Results Trap Report Style** to control the way detected stations are reported in the notification:
   - Report all detected stations since last scan (default)
   - Report all detected stations since start of scan
9. Configure the second wireless interface, if required.
10. Click **OK**.

The results of the Rogue Scan can be viewed in the **Status** page in the HTTP interface.

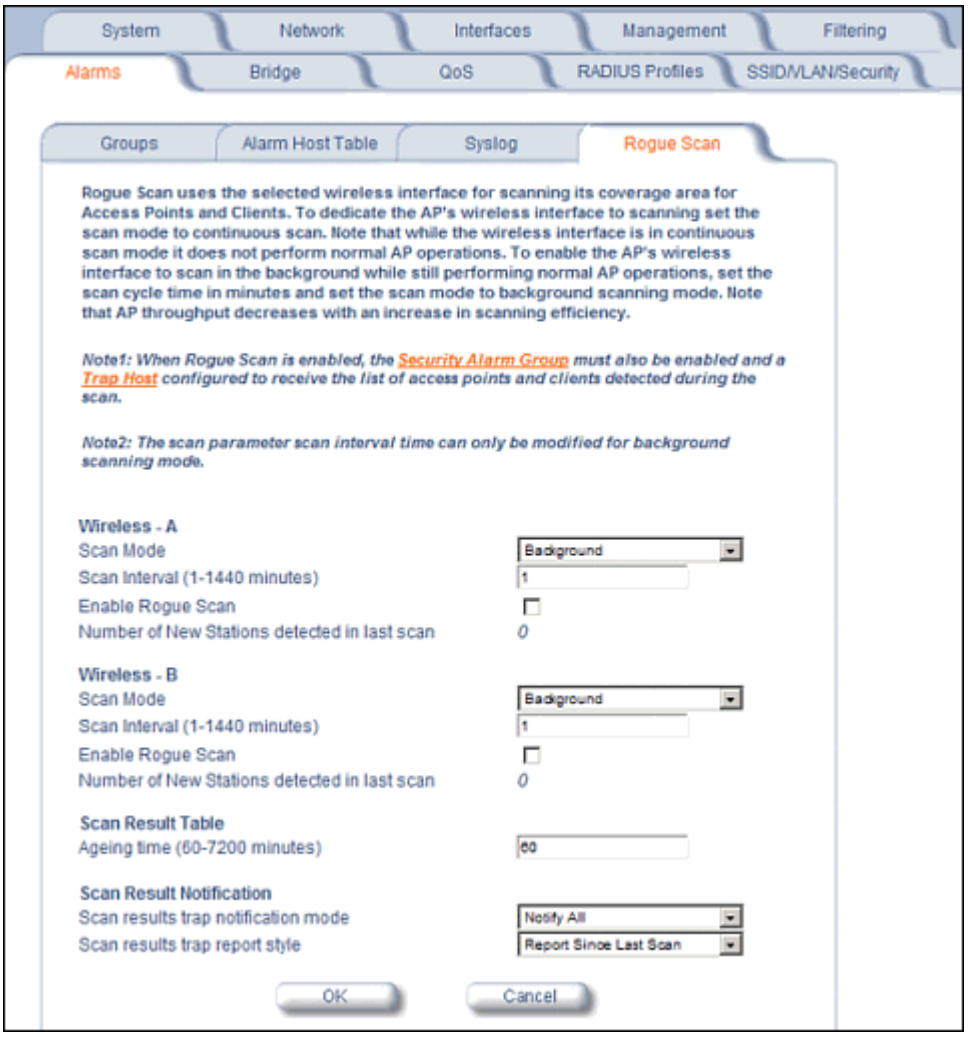


Figure 4-28 Rogue Scan Screen

Bridge

The AP is a bridge between your wired and wireless networking devices. As a bridge, the functions performed by the AP include:

- MAC address learning
- Forward and filtering decision making
- Spanning Tree protocol used for loop avoidance

Once the AP is connected to your network, it learns which devices are connected to it and records their MAC addresses in the Learn Table. The table can hold up to 10,000 entries. To view the Learn Table, click on the **Monitor** button in the web interface and select the Learn Table tab.

The **Bridge** tab has four sub-tabs:

- Spanning Tree
- Intra BSS
- Packet Forwarding

Spanning Tree

A Spanning Tree is used to avoid redundant communication loops in networks with multiple bridging devices. Bridges do not have any inherent mechanism to avoid loops, because having redundant systems is a necessity in certain networks. However, redundant systems can cause Broadcast Storms, multiple frame copies, and MAC address table instability problems.

Complex network structures can create multiple loops within a network. The Spanning Tree configuration blocks certain ports on AP devices to control the path of communication within the network, avoiding loops and following a spanning tree structure.

For more information on Spanning Tree protocol, please see Section 8.0 of the IEEE 802.1d standard. The Spanning Tree configuration options are advanced settings. Proxim recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

NOTE: *Spanning Tree protocol does not run on Mesh ports.*

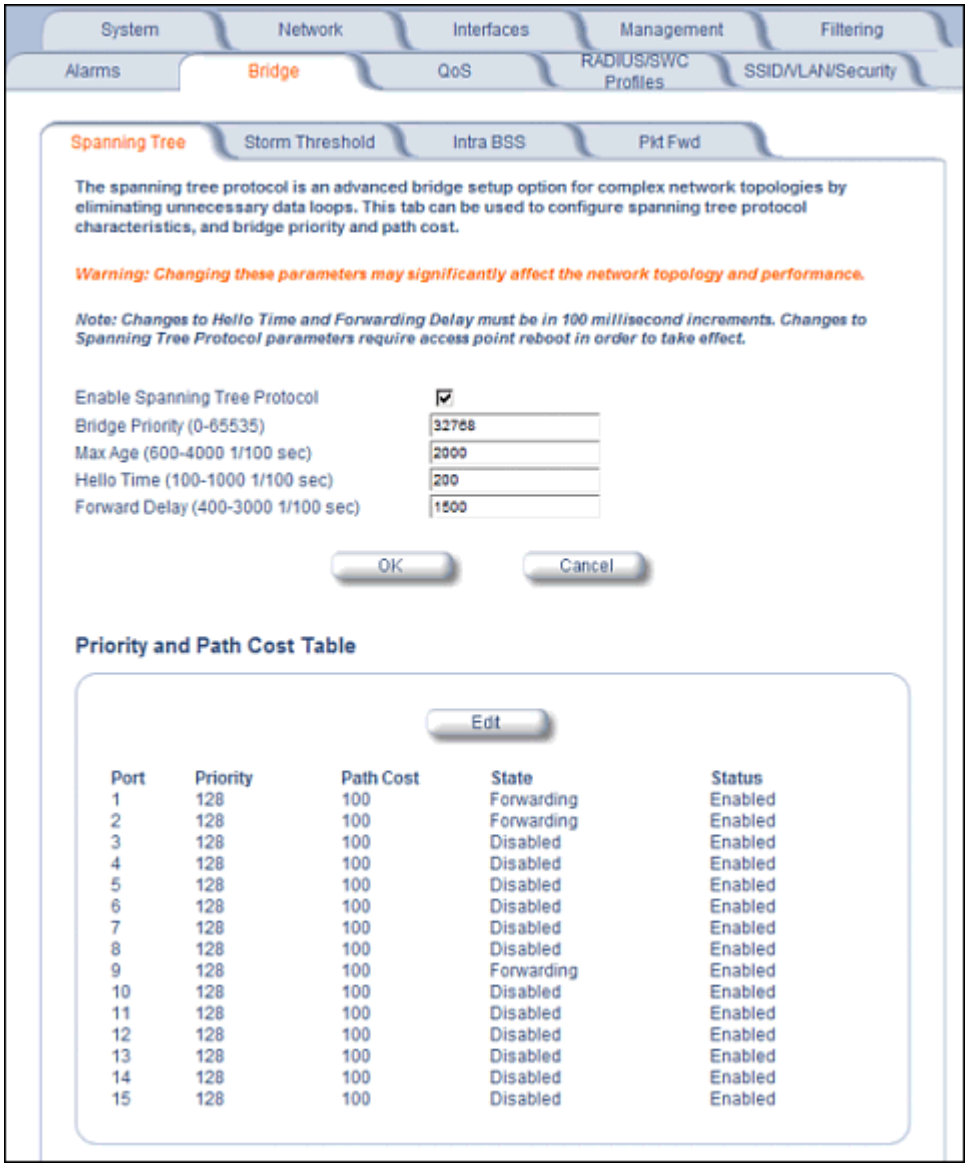


Figure 4-29 Spanning Tree Sub-Tab

Storm Threshold

Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- Specifying an absolute maximum number of messages per interface.

The Storm Threshold parameters allow you to specify a set of thresholds for each interface of the AP, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for an interface or from a single network device exceeds the maximum value per second, the AP will ignore all subsequent messages in that second received on that interface or from that network device.

- **Address Threshold:** Enter the maximum allowed number of packets per second.
- **Ethernet Threshold:** Enter the maximum allowed number of packets per second.

- **Wireless Threshold:** Enter the maximum allowed number of packets per second.

Intra BSS

The wireless clients (or *subscribers*) that associate with a certain AP form the Basic Service Set (BSS) of a network infrastructure. By default, wireless subscribers in the same BSS can communicate with each other. However, some administrators (such as wireless public spaces) may wish to block traffic between wireless subscribers that are associated with the same AP to prevent unauthorized communication and to conserve bandwidth. This feature enables you to prevent wireless subscribers within a BSS from exchanging traffic.

Although this feature is generally enabled in public access environments, Enterprise LAN administrators use it to conserve wireless bandwidth by limiting communication between wireless clients. For example, this feature prevents peer-to-peer file sharing or gaming over the wireless network.

To block Intra BSS traffic, set **Intra BSS Traffic Operation** to **Block**.

To allow Intra BSS traffic, set **Intra BSS Traffic Operation** to **Passthru**.

Packet Forwarding

The Packet Forwarding feature enables you to redirect traffic generated by wireless clients that are all associated to the same AP to a single MAC address. This filters wireless traffic without burdening the AP and provides additional security by limiting potential destinations or by routing the traffic directly to a firewall. You can redirect to a specific port (Ethernet or WDS) or allow the bridge's learning process (and the forwarding table entry for the selected MAC address) to determine the optimal port.

NOTE: *The gateway to which traffic will be redirected should be node on the Ethernet network. It should not be a wireless client.*

Configuring Interfaces for Packet Forwarding

Configure your AP to forward packets by specifying port(s) to which packets are redirected and a destination MAC address.

1. Within the ***Packet Forwarding Configuration*** screen, check the box labeled **Enable Packet Forwarding**.
2. Specify a destination **Packet Forwarding MAC Address**. The AP will redirect all unicast, multicast, and broadcast packets received from wireless clients to the address you specify.
3. Select a **Packet Forwarding Interface Port** from the drop-down menu. You can redirect traffic to:
   – Ethernet
   – A WDS connection (see Wireless Distribution System (WDS) for details)
   – Any (traffic is redirected to a port based on the bridge learning process)
4. Click **OK** to save your changes.

QoS

Wireless Multimedia Extensions (WME)/Quality of Service (QoS)

The AP supports Wireless Multimedia Enhancements which defines an intermediate solution for QoS functionality until the IEEE 802.11e specification is formally approved. WME is based on a subset of the 802.11e standard, and defines enhancements to the MAC for wireless LAN applications with Quality of Service requirements, which include transport of voice traffic over IEEE 802.11 wireless LANs.

The enhancement are in the form of changes in protocol frame formats (addition of new fields and information elements), addition of new messages, definition of new protocol actions, channel access mechanisms (differentiated control of access to medium) and network elements (QoS/WME aware APs, STAs), and configuration management.

WME supports Enhanced Distributed Channel Access (EDCA) for prioritized QoS services. The WME/QoS feature can be enabled or disabled per wireless interface. For more information on QoS, see “Technical Bulletin 69504 Revision 2” at <http://keygen.proxim.com/support/orinoco/tb/tb69504_3wmm.pdf>.

Enabling QoS and Adding QoS policies

Perform the following procedure to enable QoS and add QoS policies:

1. Click **Configure > QoS > Policy**.

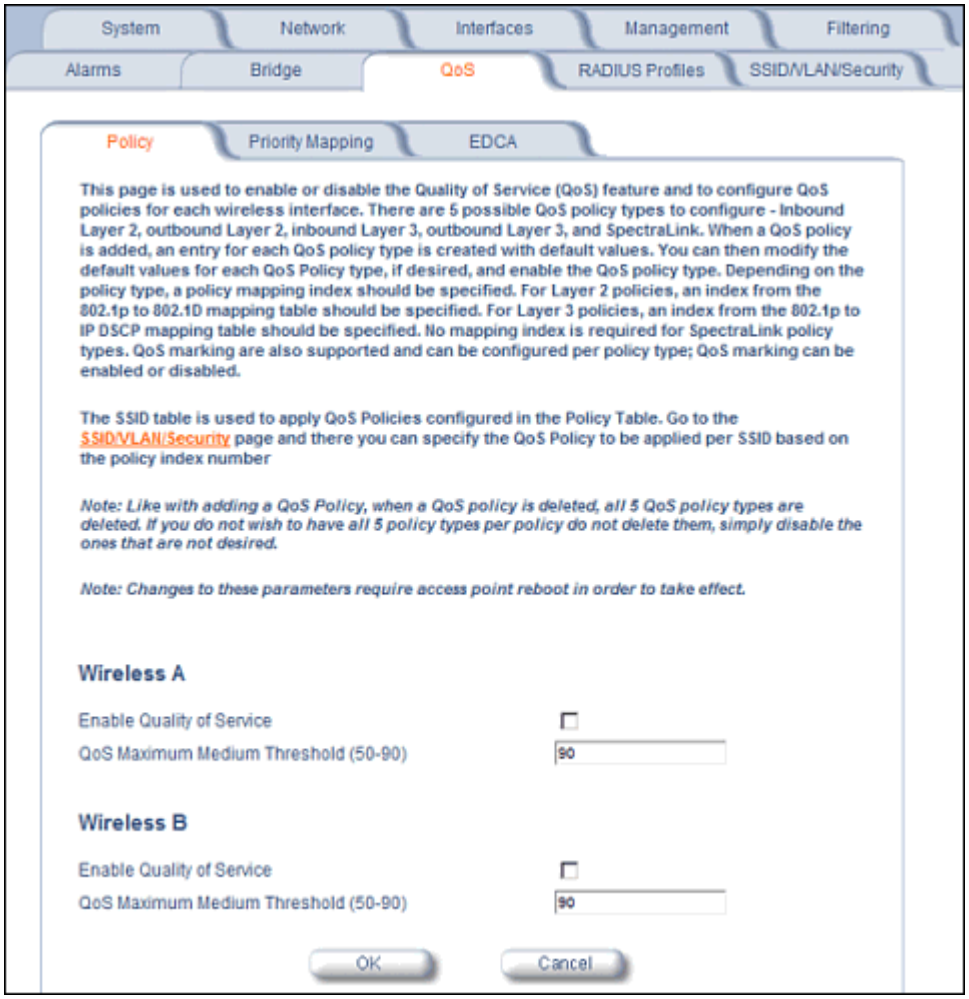


Figure 4-30 QoS Policies

2. To enable QoS, check the **Enable Quality of Service** checkbox.
3. Configure the **QoS Maximum Medium Threshold** for all Admission Controls. Admission will be granted if the new requested traffic stream and already admitted time is less than the *medium maximum threshold*.
4. To add a QoS Policy, click the **Add** button in the “QoS Policies Table” box. The Add Entries box appears.

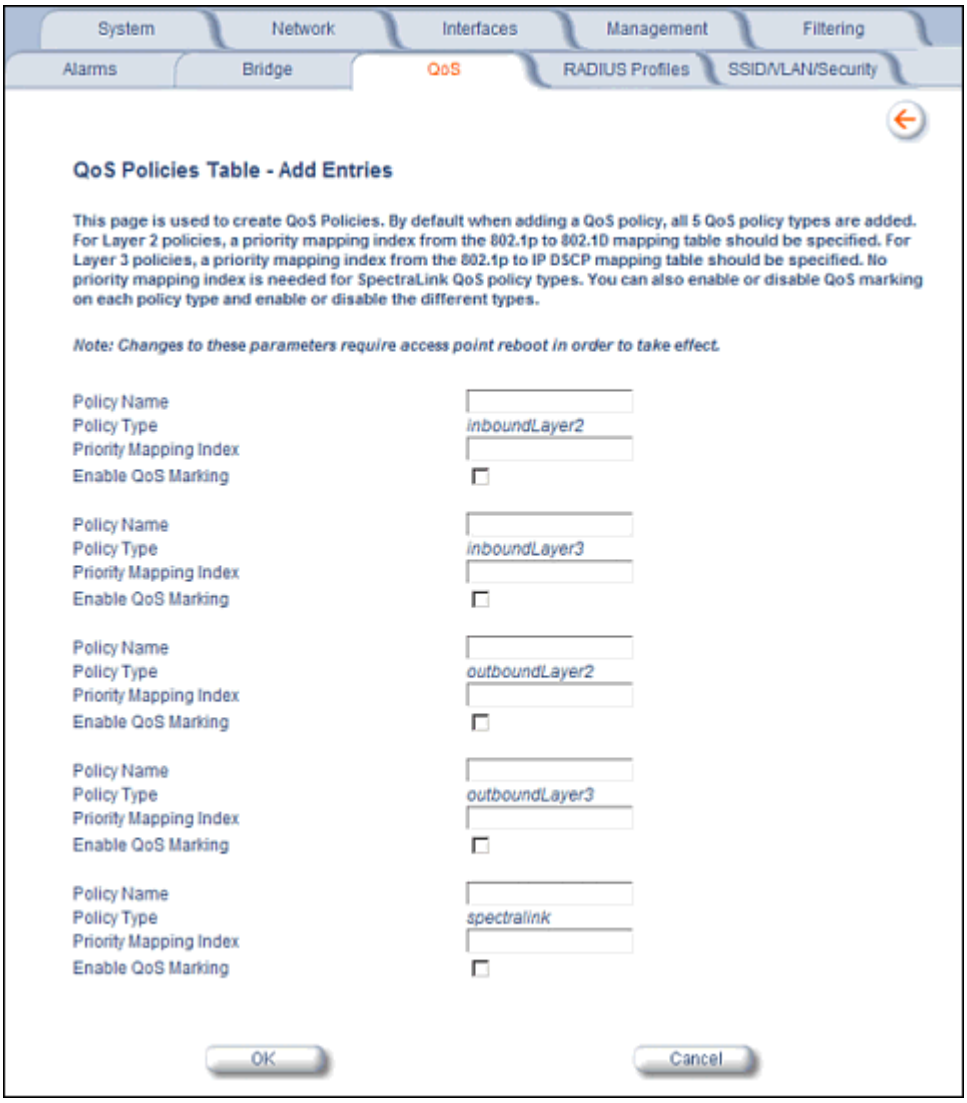


Figure 4-31 Add QoS Policy

5. Enter the **Policy Name**.
6. Select the **Policy Type**:
   - **inlayer2**: inbound traffic direction, Layer 2 traffic type
   - **inlayer3**: inbound traffic direction, Layer 3 traffic type
   - **outlayer2**: outbound traffic direction, Layer 2 traffic type
   - **outlayer3**: inbound traffic direction, Layer 3 traffic type
   - **spectralink**: SpectraLink traffic
7. Enter the **Priority Mapping Index**.

   For layer 2 policies, an index from the 802.1p to 802.1d mapping table should be specified. For layer 3 policies, an index from the 802.1p to IP DSCP mapping table should be specified. No mapping index is required for SpectraLink.

8. Select whether to **Enable QoS Marking**.
9. Click **OK**.

Priority Mapping

Use this page to configure QoS 802.1p to 802.1d priority mappings (for layer 2 policies) and IP DSCP to 802.1d priority mappings (for layer 3 policies). The first entry in each table contains the recommended priority mappings. Custom entries can be added to each table with different priority mappings.

1. Click **Configure > QoS > Priority Mapping**.

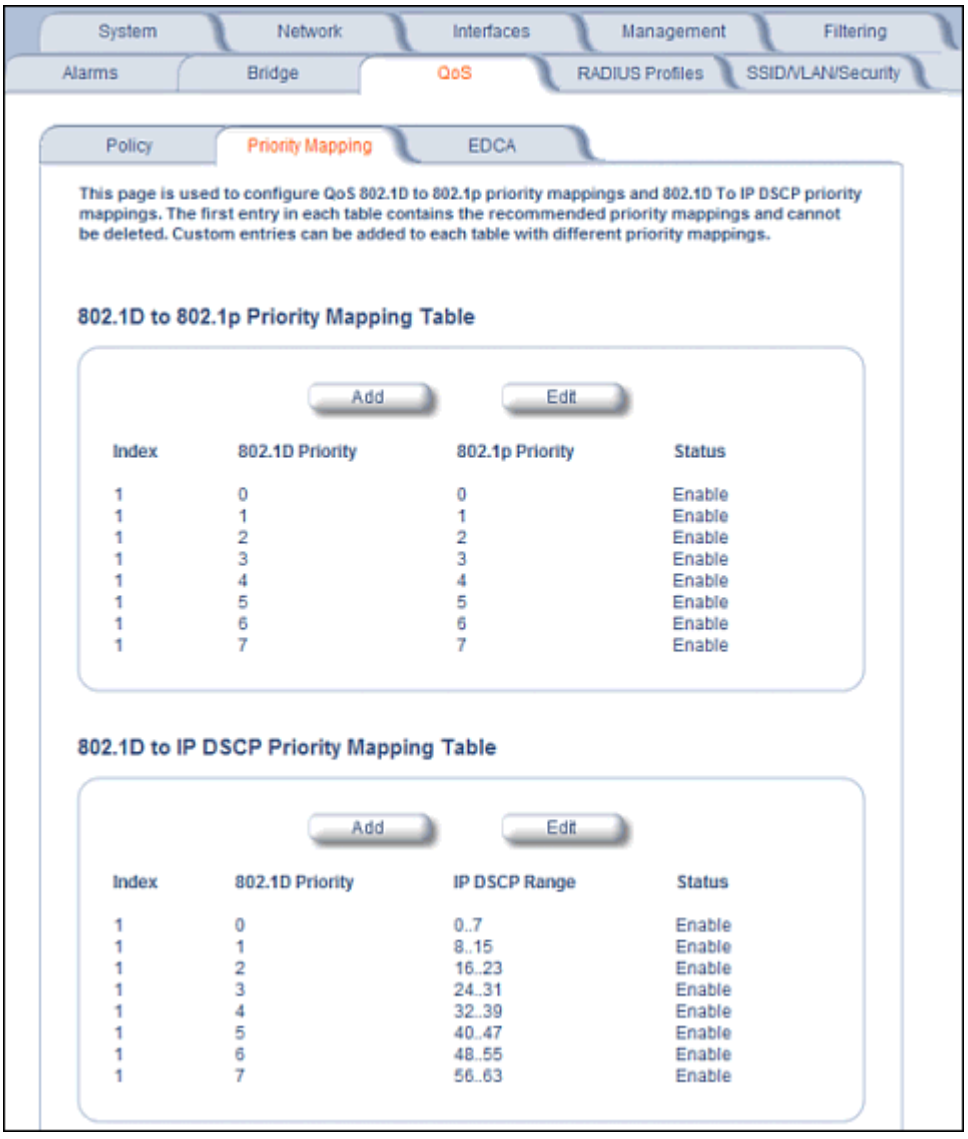


Figure 4-32 Priority Mapping

2. Click **Add** in the 802.1p and 802.1d priority mapping table.

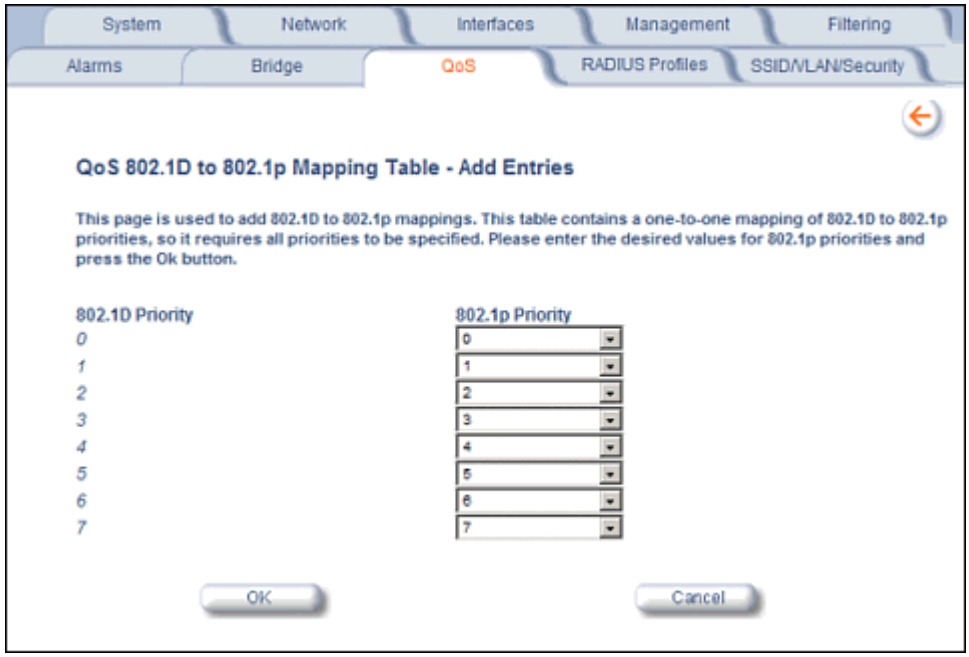


Figure 4-33 Add Priority Mapping Entry

3. Select the 802.1p Priority (from 0-7) for 802.1d Priorities 0-7.
4. Click **OK**.
5. Click **Add** in the IP Precedence/DSCP ranges and 802.1d Priority table.
6. Select the IP DSCP Range for each 802.1d Priority.
7. Click **OK**.

NOTE: *Changes to Priority Mapping require a reboot of the AP to take effect.*

Enhanced Distributed Channel Access (EDCA)

WME uses Enhanced Distributed Channel Access, a prioritized CSMA/CA access mechanism used by WME-enabled clients/AP in a WME enabled BSS to realize different classes of differentiated Channel Access.

A wireless Entity is defined as all wireless clients and APs in the wireless medium contending for the common wireless medium. EDCA uses a separate channel access function for each of the Access Categories (Index) within a wireless entity. Each channel access function in a wireless entity that contends for the wireless medium as if it were a separate client contending for the wireless medium. Different channel access functions in a given Wireless Entity contend among themselves for access to the wireless medium in addition to contending with other clients.

STA EDCA Table and AP EDCA Table

This page is used to configure the client (STA) and AP Enhanced Distributed Channel Access (EDCA) parameters. You can modify the EDCA values for both Wireless A and Wireless B.

The EDCA parameter set provides information needed by the client stations for proper QoS operation during the wireless contention period. These parameters are used by the QoS enabled AP to establish policy, to change policies when accepting new stations or new traffic, or to adapt to changes in the offered load. The EDCA parameters assign priorities to traffic types where higher priority packets gain access to the wireless medium more frequently than lower priority packets.

NOTE: *Default recommended values for EDCA parameters have been defined; Proxim recommends not modifying EDCA parameters unless strictly necessary.*

Perform the following procedure to configure the Station and AP EDCA tables.

1. Click **Configure > QoS > EDCA**.

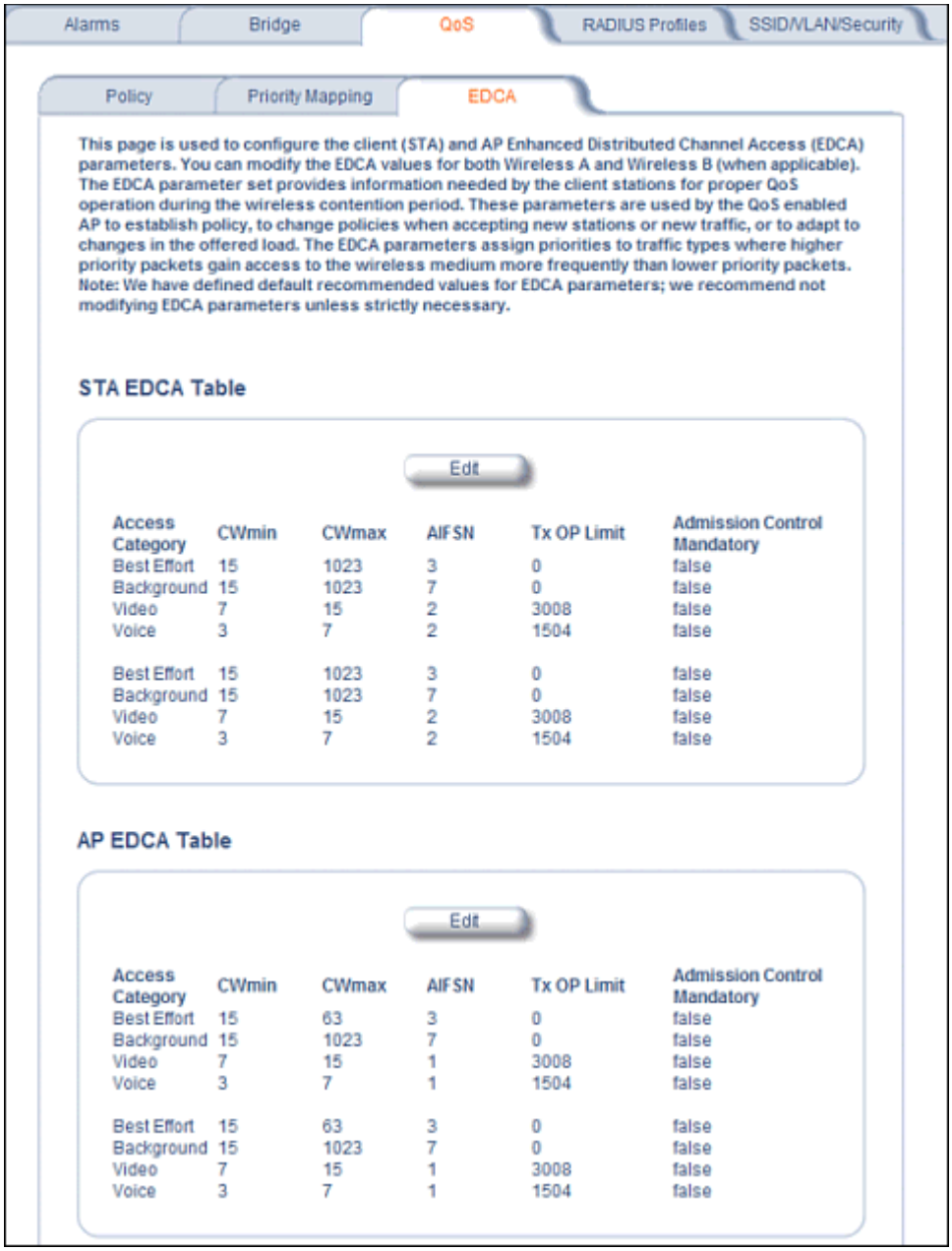


Figure 4-34 EDCA Tables

2. Click **Edit** and configure the following parameters in each table:

   NOTE: *Changes to EDCA parameters require a reboot of the AP to take effect.*

   - **Index**: read-only. Indicates the index of the Access Category (1-4) being defined.
   - **CWMin**: minimum Contention Window. Configurable range is 0 to 255.
   - **CWMax**: maximum Contention Window. Configurable range is 0 to 65535.
   - **AIFSN**: Arbitration IFS per access category. Configurable range is 2 to 15.

- **Tx OP Limit**: The Transmission Opportunity Limit. The Tx OP is an interval of time during which a particular QoS enhanced client has the right to initiate a frame exchange sequence onto the wireless medium. The Tx OP Limit defines the upper limit placed on the value of Tx OP a wireless entity can obtain for a particular access category. Configurable range is 0 to 65535.
- **MSDU Lifetime**: specifies the maximum elapsed time between a MSDU transfer request and delivery to the destination, beyond which delivery becomes unnecessary. Configurable range is 0 to 500 seconds.
- **Admission Control Mandatory**: Possible values are True or False. Admission control defines if an Access Point accepts or rejects a requested traffic stream with certain QoS specifications, based on available channel capacity and link conditions. Admission control can be configured for each Access Category (Index).
  On the Policy sub-tab, the user can also configure a *medium maximum threshold* for all Admission Controls. Admission will be granted if the new requested traffic stream and already admitted time is less than the *medium maximum threshold*.

Radius Profiles

Configuring Radius Profiles on the AP allows the administrator to define a profile for RADIUS Servers used by the system or by a VLAN. The network administrator can define RADIUS Servers per Authentication Mode and per VLAN.

The AP communicates with the RADIUS server defined in a profile to provide the following features:

- MAC Access Control Via RADIUS Authentication
- 802.1x Authentication using RADIUS
- RADIUS Accounting

Also, RADIUS Based Management Access allows centralized user management.

The network administrator can configure default RADIUS authentication servers to be used on a system-wide basis, or in networks with VLANs enabled the administrator can also configure separate authentication servers to be used for MAC authentication, EAP authentication, or Accounting in each VLAN. You can configure the AP to communicate with up to six different RADIUS servers per VLAN/SSID:

- Primary Authentication Server (MAC-based authentication)
- Back-up Authentication Server (MAC-based authentication)
- Primary Authentication Server (EAP/802.1x authentication)
- Back-up Authentication Server (EAP/802.1x authentication)
- Primary Accounting Server
- Back-up Accounting Server

The back-up servers are optional, but when configured, the AP will communicate with the back-up server if the primary server is off-line. After the AP has switched to the backup server, it will periodically check the status of the primary RADIUS server every five (5) minutes. Once the primary RADIUS server is again online, the AP automatically reverts from the backup RADIUS server back to the primary RADIUS server. All subsequent requests are then sent to the primary RADIUS server.

You can view monitoring statistics for each of the configured RADIUS servers.

RADIUS Servers per Authentication Mode and per VLAN

The user can configure separate RADIUS authentication servers for each authentication mode and for each SSID (VLAN). For example:

- The user can configure separate RADIUS servers for RADIUS MAC authentication and 802.1x authentication
- The user can configure separate RADIUS servers for each VLAN: VLAN1 could support only WEP clients, whereas VLAN2 could support 802.1x and WEP clients.

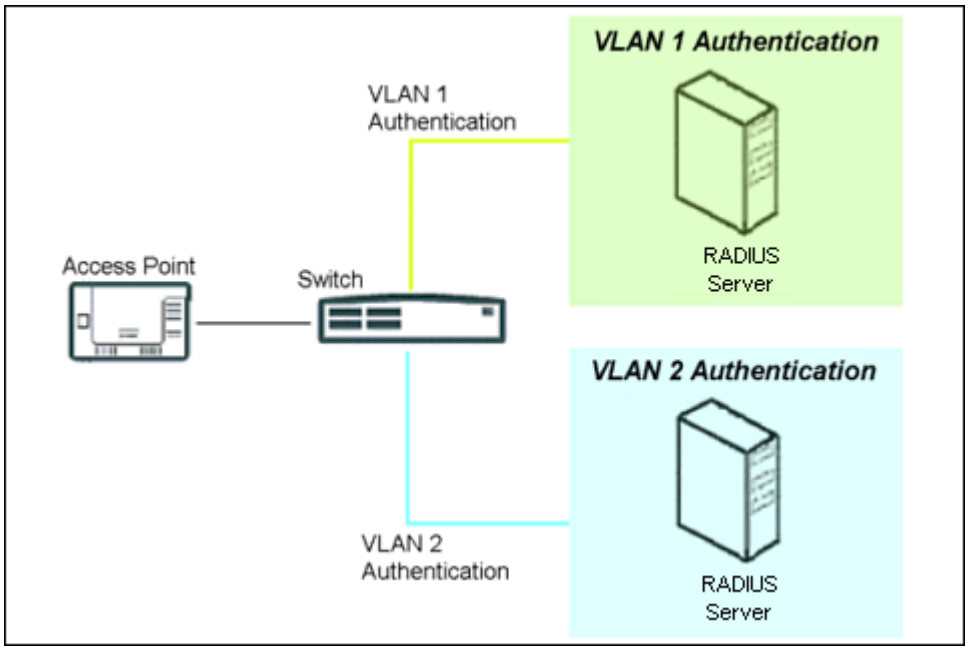


Figure 4-35 RADIUS Servers per VLAN

This figure shows a network with separate authentication servers for each authentication type and for each VLAN. The clients in VLAN 1 are authenticated using the authentication servers configured for VLAN 1. The type of authentication server used depends on whether the authentication is done for an 802.1x client or a non-802.1x client. The clients in VLAN 2 are authenticated using a different set of authentication servers configured for authenticating users in VLAN 2.

Authentication servers for each VLAN are configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, “MAC Authentication”, “EAP Authentication”, Accounting”, and “Management”.

RADIUS Servers Enforcing VLAN Access Control

A RADIUS server can be used to enforce VLAN access control in two ways:

- Authorize the SSID the client uses to connect to the AP. The SSID determines the VLAN that the client gets assigned to.
- Assigning the user to a VLAN by specifying the VLAN membership information of the user.

Configuring Radius Profiles

A RADIUS server Profile consists of a Primary and a Secondary RADIUS server that get assigned to act as either MAC Authentication servers, 802.1x/EAP Authentication servers, or Accounting Servers in the VLAN Configuration. See Configuring Security Profiles.

The RADIUS Profiles Sub-tab allows you to add new RADIUS profiles or modify or delete existing profiles.

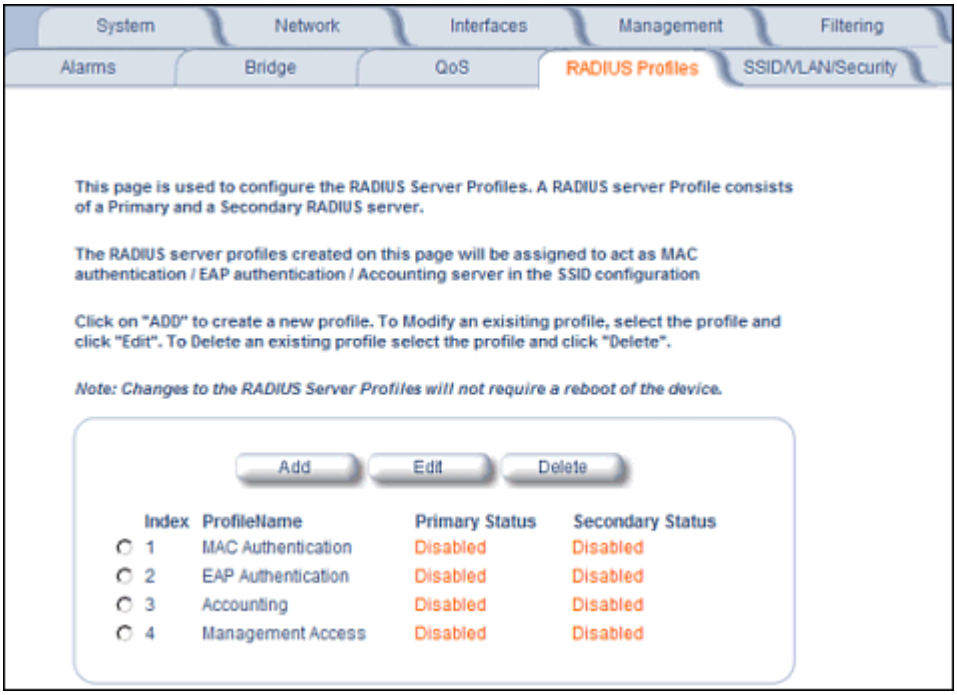


Figure 4-36 RADIUS Server Profiles

Adding or Modifying a RADIUS Server Profile

Perform the following procedure to add a RADIUS server profile and to configure its parameters.

1. Click **Add** to create a new profile. To Modify an existing profile, select the profile and click Edit. To delete an existing profile, select the profile and click Delete. You cannot delete a RADIUS server profile if it is applied to an SSID.
2. Configure the following parameters for the RADIUS Server profile (see Figure 4-37):

NOTE: *This page configures only the Primary RADIUS Server associated with the profile. After configuring these parameters, save them by clicking OK. Then, to configure the Secondary RADIUS Server, edit the profile from the main page.*

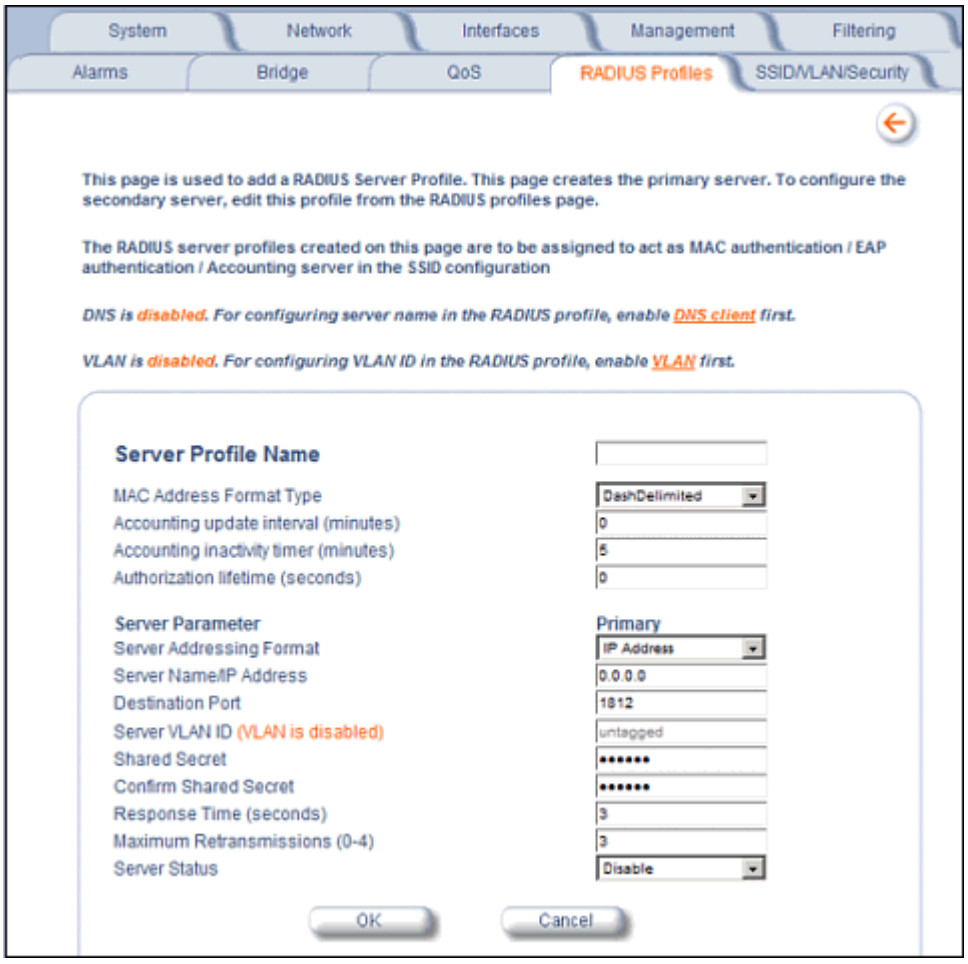


Figure 4-37 Add RADIUS Server Profile

- **Server Profile Name**: the profile name. This is the name used to associated a VLAN to the profile. See Configuring Security Profiles. The Server Profile Name is also used in the Configure > Management > Services page to specify the RADIUS profile to be used for RADIUS Based Management Access.
- **MAC Address Format Type**: This parameter should correspond to the format in which the clients' 12-digit MAC addresses are listed within the RADIUS server. Available options are:
  - — Dash delimited: dash between each pair of digits: xx-yy-zz-aa-bb-cc
  - — Colon delimited: colon between each pair of digits: xx:yy:zz:aa:bb:cc
  - — Single dash delimited: dash between the sixth and seventh digits: xxyyzz-aabbcc
  - — No delimiters: No characters or spaces between pairs of hexadecimal digits: xxyyzzaabbcc
- **Accounting update interval:** Enter the time interval (in minutes) for sending Accounting Update messages to the RADIUS server. A value of 0 (default) means that the AP will not send Accounting Update messages.
- **Accounting inactivity timer:** Enter the accounting inactivity timer. This parameter supports a value from 1-60 minutes. The default is 5 minutes.
- **Authorization lifetime**: Enter the time, in seconds, each client session may be active before being automatically re-authenticated. This parameter supports a value between 900 and 43200 seconds. The default is 0 (disabled).
- **Server Addressing Format:** select IP Address or Name. If you want to identify RADIUS servers by name, you must configure the AP as a DNS Client. See DNS Client for details.
- **Server Name/IP Address:** Enter the server's name or IP address.

- **Destination Port:** Enter the port number which the AP and the server will use to communicate. By default, RADIUS servers communicate on port 1812.
- **Server VLAN ID**: Indicates the VLAN that uses this RADIUS server profile. If VLAN is disabled, this field will be grayed out.
- **Shared Secret and Confirm Shared Secret:** Enter the password shared by the RADIUS server and the AP. The same password must also be configured on the RADIUS server. The default password is “public.”
- **Response Time (seconds)**: Enter the maximum time, in seconds, that the AP should wait for the RADIUS server to respond to a request. The range is 1-10 seconds; the default is 3 seconds.
- **Maximum Retransmissions (0-4)**: Enter the maximum number of times an authentication request may be transmitted. The range is 0 to 4, the default is 3.
- **Server Status**: Select Enable from the drop-down box to enable the RADIUS Server Profile.

3. Click **OK**.
4. Select the Profile and click **Edit** to configure the Secondary RADIUS Server, if required.

MAC Access Control Via RADIUS Authentication

If you want to control wireless access to the network and if your network includes a RADIUS Server, you can store the list of MAC addresses on the RADIUS server rather than configure each AP individually. You can define a RADIUS Profile that specifies the IP Address of the server that contains a central list of MAC Address values identifying the authorized stations that may access the wireless network. You must specify information for at least the primary RADIUS server. The back-up RADIUS server is optional.

NOTE: *Each VLAN can be configured to use a separate RADIUS server (and backup server) for MAC authentication. MAC access control can be separately enabled for each VLAN.*

NOTE: *Contact your RADIUS server manufacturer if you have problems configuring the server or have problems using RADIUS authentication.*

802.1x Authentication using RADIUS

You must configure a primary EAP/802.1x Authentication server to use 802.1x security. A back-up server is optional.

NOTE: *Each VLAN can be configured to use a separate RADIUS server (and backup server) for 802.1x authentication. 802.1x authentication (“EAP authentication”) can be separately enabled for each VLAN.*

RADIUS Accounting

Using an external RADIUS server, the AP can track and record the length of client sessions on the access point by sending RADIUS accounting messages per RFC2866. When a wireless client is successfully authenticated, RADIUS accounting is initiated by sending an “Accounting Start” request to the RADIUS server. When the wireless client session ends, an “Accounting Stop” request is sent to the RADIUS server.

NOTE: *Each VLAN can be configured to use a separate RADIUS accounting server (and backup accounting server).*

Session Length

Accounting sessions continue when a client reauthenticates to the same AP. Sessions are terminated when:

- A client disassociates.
- A client does not transmit any data to the AP for a fixed amount of time.
- A client is detected on a different interface.
- Idle-Timeout or Session-Timeout attributes are configured in the Radius server.

If the client roams from one AP to another, one session is terminated and a new session is begun.

NOTE: *This feature requires RADIUS authentication using MAC Access Control or 802.1x. Wireless clients configured in the Access Point's static MAC Access Control list are not tracked.*

Authentication and Accounting Attributes

Additionally, the AP supports a number of Authentication and Accounting Attributes defined in RFC2865, RFC2866, RFC2869, and RFC3580.

Authentication Attributes

- State: Received in Access-Accept Packet by the AP during Authentication and sent back as-is during Re-Authentication.
- Class: Received in Access-Accept Packet by the AP during Authentication and back as in Accounting Packets.
- Session-Timeout
  - If the RADIUS server does not send a Session-Timeout, the AP will set the subscriber expiration time to 0, which means indefinite access.
  - The Termination Action attribute defines how the Session-Timeout attribute will be interpreted. If the Termination Action is DEFAULT, then the session is terminated on expiration of the Session-Timeout time interval. If Termination Action is RADIUS-Request, then re-authentication is done on expiration on the session.
  - If the RADIUS server sends a Session-Timeout, the value specified by the Session-Timeout attribute will take precedence over the configured Authorization Lifetime value.
- Termination-Action
  - Valid values are: Default (0), RADIUS-Request (1). When the value is "default," the Termination-Action attribute sends an accounting stop message and then reauthenticates. If the value is "RADIUS-Request," the Termination-Action attribute reauthenticates without sending an accounting stop.
- Idle Timeout
  - The AP internally maintains the Idle-Timeout attribute obtained for each of the users during their authentication process, and uses this time interval in place of accounting inactivity time for timing out clients.
- Calling Station Id
  - MAC address of the client getting authenticated.
- Called Station Id
  - The AP sends the MAC address of its own wireless interface with which the client getting authenticated is getting associated, appended with the SSID. If VLAN is enabled, the SSID and corresponding VLAN ID get appended.
- Acct-Interim-Interval
  - Obtained during the Authentication process and used for determining the time interval for sending Accounting Update messages.
  - This attribute value takes precedence over the value of the Accounting Update Interval.

Accounting Attributes

- Acct-Delay-Time
  - Indicates how many seconds the AP has been trying to send a particular packet related to a particular user. This time can be used at the server to determine the approximate time of the event generating this accounting request.
- Acct-Session-Id
  - Unique accounting ID that aids in tracking client accounting records. This attribute is sent in Start and Stop RADIUS accounting messages, and contains the client MAC address appended with the unique session ID.
- Acct-Session-Time
  - Acct-Session-Time is calculated the following way (for each transmitted/retransmitted Acct-Stop): Acct-Session-Time = time of last sent packet - subscriber login time.
- Acct-Input-Octets

  - Number of octets (bytes) received by subscriber.
- Acct-Output-Octets
  - Number of octets (bytes) sent by subscriber.
- Acct-Input-Packets
  - Number of packets received by subscriber.
- Acct-Output-Packets
  - Number of packets sent by subscriber.
- Acct-Terminate Cause
  - Indicates how the session was terminated.
- Vendor Specific Attributes

SSID/VLAN/Security

The AP provides several security features to protect your network from unauthorized access. This section gives an overview of VLANs and then discusses the SSID/VLAN/Security configuration options in the AP:

- VLAN Overview
- Management VLAN
- Security Profile
- MAC Access
- Wireless-A or Wireless-B

The AP also provides Broadcast SSID/Closed System and Rogue Scan to protect your network from unauthorized access. See the Broadcast SSID and Closed System and Rogue Scan sections from more information.

VLAN Overview

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to clients) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

AP devices are fully VLAN-ready; however, by default VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
  - Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own VLAN
  - Clients roam without compromising security

VLAN tagged data is collected and distributed through an AP's wireless interface(s) based on Network Name (SSID). An Ethernet port on the access point connects a wireless cell or network to a wired backbone. The access points communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses for the VLAN(s). Resources like servers and printers may be present, and a hub may include multiple APs, extending the network over a larger area.

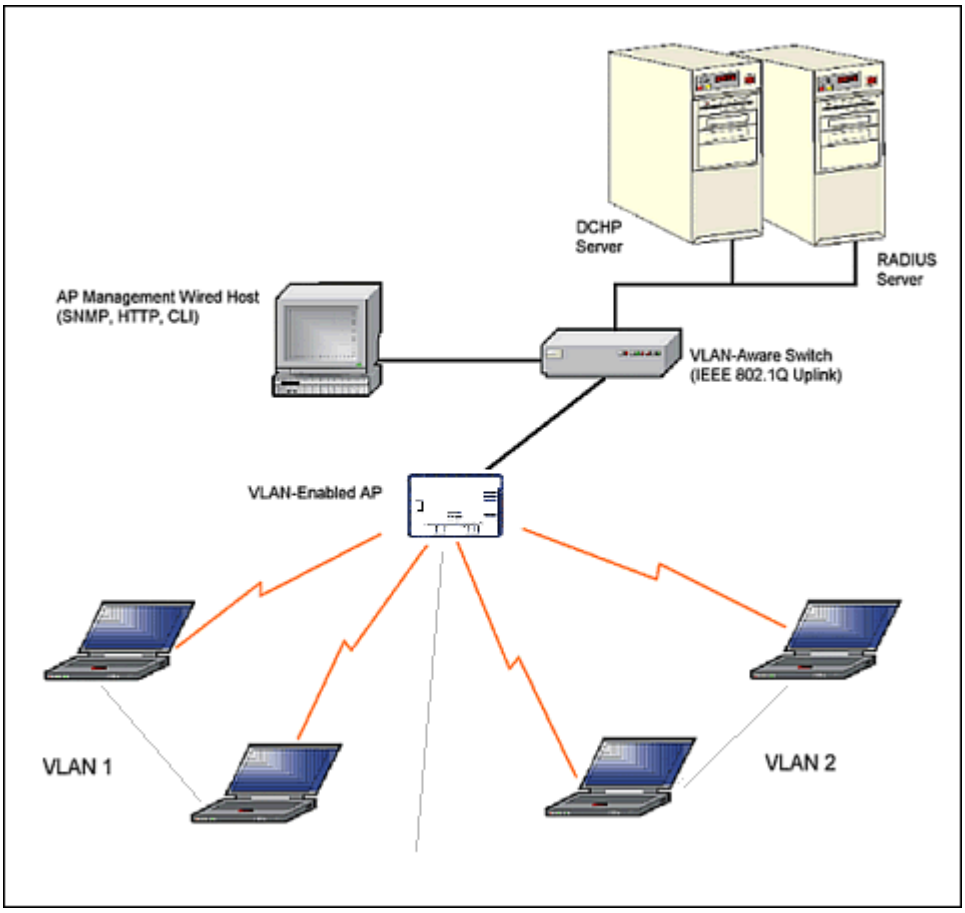


Figure 4-38 Components of a Typical VLAN

VLAN Workgroups and Traffic Management

Access Points that are not VLAN-capable typically transmit broadcast and multicast traffic to all wireless Network Interface Cards (NICs). This process wastes wireless bandwidth and degrades throughput performance. In comparison, a VLAN-capable AP is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 16 SSIDs per radio, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup; for example, one VLAN could be used for an EMPLOYEE workgroup and the other for a GUEST workgroup.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup could be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup.

The AP can segment users into a maximum of 16 different workgroups per radio, based on an SSID/VLAN grouping (also referred as a VLAN Workgroup or a Sub-network).

The primary scenarios for using VLAN workgroups are as follows:

1. VLAN disabled: Your network does not use VLANs, and you cannot configure the AP to use multiple SSIDs.
2. VLAN enabled, each VLAN workgroup uses a different VLAN ID Tag.
3. VLAN enabled, a mixture of Tagged and Untagged workgroups exist.
4. VLAN enabled, all VLANs untagged: VLAN is enabled in order to use SSID. (Note that typical use of SSIDs assumes actual use of VLANs.)

NOTE: *VLAN must be enabled to configure security per SSID.*

Management VLAN

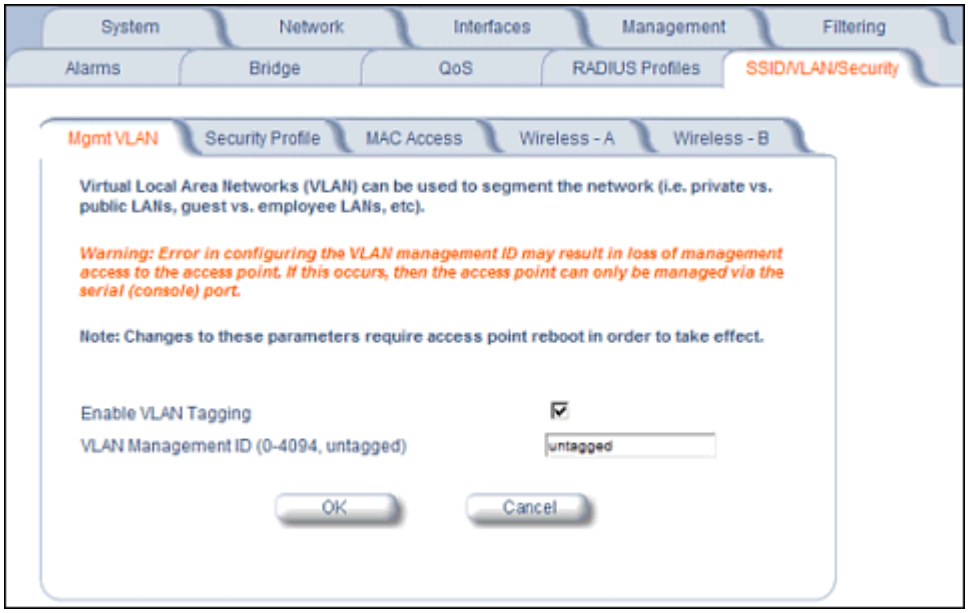


Figure 4-39 Mgmt VLAN

VLAN Tagging Management

Control Access to the AP

Management access to the AP can easily be secured by making management stations or hosts and the AP itself members of a common VLAN. Simply configure a non-zero management VLAN ID and enable VLAN to restrict management of the AP to members of the same VLAN.

CAUTION: *If a non-zero management VLAN ID is configured then management access to the AP is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the AP.*

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Set the VLAN Management ID to a value of between 1 and 4094. (A value of -1 disables VLAN Tagging).

3. Place a check mark in the **Enable VLAN Tagging** box.

Provide Access to a Wireless Host in the Same Workgroup

The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN User ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION: *Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.*

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Set the **VLAN Management ID** to use the same VLAN ID as one of the configured SSIDs.
3. Place a check mark in the **Enable VLAN Tagging** box.

Disable VLAN Tagging

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Remove the check mark from the **Enable VLAN Tagging** box (to disable all VLAN functionality) or set the **VLAN Management ID** to -1 (to disable VLAN Tagging only).

NOTE: *If you disable VLAN Tagging, you will be unable to configure security per SSID.*

Security Profile

The AP supports the following security features:

- WEP Encryption: The original encryption technique specified by the IEEE 802.11 standard.
- 802.1x Authentication: An IEEE standard for client authentication.
- Wi-Fi Protected Access (WPA/802.11i [WPA2]): A new standard that provides improved encryption security over WEP.

NOTE: *The AP does not support shared key 802.11 MAC level authentication. Clients with this MAC level feature must disable it.*

WEP Encryption

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

802.1x Authentication

IEEE 802.1x is a standard that provides a means to authenticate and authorize network devices attached to a LAN port. A port in the context of IEEE 802.1x is a point of attachment to the LAN, either a physical Ethernet connection or a wireless link to an Access Point. 802.1x requires a RADIUS server and uses the Extensible Authentication Protocol (EAP) as a standards-based authentication framework, and supports automatic key distribution for enhanced security. The EAP-based authentication framework can easily be upgraded to keep pace with future EAP types.

Popular EAP types include:

- EAP-Message Digest 5 (MD5): Username/Password-based authentication; does not support automatic key distribution
- EAP-Transport Layer Security (TLS): Certificate-based authentication (a certificate is required on the server and each client); supports automatic key distribution

- EAP-Tunneled Transport Layer Security (TTLS): Certificate-based authentication (a certificate is required on the server; a client's username/password is tunneled to the server over a secure connection); supports automatic key distribution
- PEAP - Protected EAP with MS-CHAP: Secure username/password-based authentication; supports automatic key distribution

Different servers support different EAP types and each EAP type provides different features. See the documentation that came with your RADIUS server to determine which EAP types it supports.

NOTE: *The AP supports the following EAP types when Security Mode is set to 802.1x, WPA, or 802.11i (WPA2): EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, and EAP-SIM.*

Authentication Process

There are three main components in the authentication process. The standard refers to them as:

1. Supplicant (client PC)
2. Authenticator (Access Point)
3. Authentication server (RADIUS server)

When the Security Mode is set to 802.1x Station, WPA Station, or 802.11i Station you need to configure your RADIUS server for authentication purposes.

Prior to successful authentication, an unauthenticated client PC cannot send any data traffic through the AP device to other systems on the LAN. The AP inhibits all data traffic from a particular client PC until the client PC is authenticated. Regardless of its authentication status, a client PC can always exchange 802.1x messages in the clear with the AP (the client begins encrypting data after it has been authenticated).

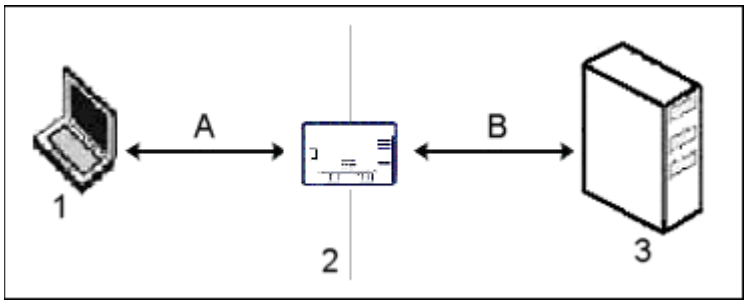


Figure 4-40 RADIUS Authentication Illustrated

The AP acts as a pass-through device to facilitate communications between the client PC and the RADIUS server. The AP (2) and the client (1) exchange 802.1x messages using an EAPOL (EAP Over LAN) protocol (A). Messages sent from the client station are encapsulated by the AP and transmitted to the RADIUS (3) server using EAP extensions (B).

Upon receiving a reply EAP packet from the RADIUS, the message is typically forwarded to the client, after translating it back to the EAPOL format. Negotiations take place between the client and the RADIUS server. After the client has been successfully authenticated, the client receives an Encryption Key from the AP (if the EAP type supports automatic key distribution). The client uses this key to encrypt data after it has been authenticated.

For 802.11a and 802.11b/g clients that communicate with an AP, each client receives its own unique encryption key; this is known as Per User Per Session Encryption Keys.

Wi-Fi Protected Access (WPA/802.11i [WPA2])

Wi-Fi Protected Access (WPA) is a security standard designed by the Wi-Fi Alliance in conjunction with the Institute of Electrical and Electronics Engineers (IEEE). The AP supports 802.11i (WPA2), based on the IEEE 802.11i security standard.

WPA is a replacement for Wired Equivalent Privacy (WEP), the encryption technique specified by the original 802.11 standard. WEP has several vulnerabilities that have been widely publicized. WPA addresses these weaknesses and provides a stronger security system to protect wireless networks.

WPA provides the following new security measures not available with WEP:

- Improved packet encryption using the Temporal Key Integrity Protocol (TKIP) and the Michael Message Integrity Check (MIC).
- Per-user, per-session dynamic encryption keys:
  - Each client uses a different key to encrypt and decrypt unicast packets exchanged with the AP
  - A client's key is different for every session; it changes each time the client associates with an AP
  - The AP uses a single global key to encrypt broadcast packets that are sent to all clients simultaneously
  - Encryption keys change periodically based on the **Re-keying Interval** parameter
  - WPA uses 128-bit encryption keys
- Dynamic Key distribution
  - The AP generates and maintains the keys for its clients
  - The AP securely delivers the appropriate keys to its clients
- Client/server mutual authentication
  - 802.1x
  - Pre-shared key (for networks that do not have an 802.1x solution implemented)

The AP supports the following WPA security modes:

- **WPA:** The AP uses 802.1x to authenticate clients and TKIP for encryption. You should only use an EAP that supports mutual authentication and session key generation, such as EAP-TLS, EAP-TTLS, and PEAP. See 802.1x Authentication for details.
- **WPA-PSK (Pre-Shared Key):** For networks that do not have 802.1x implemented, you can configure the AP to authenticate clients based on a Pre-Shared Key. This is a shared secret that is manually configured on the AP and each of its clients. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the TKIP Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).
- **802.11i** (also known as WPA2): The AP provides security to clients according to the 802.11i draft standard, using 802.1x authentication, a CCMP cipher based on AES, and re-keying.
- **802.11i-PSK** (also known as WPA2 PSK): The AP uses a CCMP cipher based on AES, and encrypts frames to clients based on a Pre-Shared Key. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).

NOTE: *For more information on WPA, see the Wi-Fi Alliance Web site at* http://www.wi-fi.org.

Authentication Protocol Hierarchy

There is a hierarchy of authentication protocols defined for the AP.

The hierarchy is as follows, from Highest to lowest:

- 802.1x authentication
- MAC Access Control via RADIUS Authentication
- MAC Access Control through individual APs' MAC Access Control Lists

  If you have both 802.1x and MAC authentication enabled, the 802.1x results will take effect. This is required in order to propagate the WEP keys to the clients in such cases. Once you disable 802.1x on the AP, you will see the effects of MAC authentication.

VLANs and Security Profiles

The AP-4000/4000M/4900M allows you to segment wireless networks into multiple sub-networks based on Network Name (SSID) and VLAN membership. A Network Name (SSID) identifies a wireless network. Clients associate with Access Points that share an SSID. During installation, the Setup Wizard prompts you to configure a Primary Network Name for each wireless interface.

After initial setup and once VLAN is enabled, the AP can be configured to support up to 16 SSIDs per wireless interface to segment wireless networks based on VLAN membership.

Each VLAN can associated to a Security Profile and RADIUS Server Profiles. A Security Profile defines the allowed wireless clients, and authentication and encryption types. See the following sections for configuration details.

Configuring Security Profiles

Security policies can be configured and applied on the AP as a whole, or on a per VLAN basis. When VLAN is disabled on the AP, the user can configure a security profile for each interface of the AP. When VLANs are enabled and Security per SSID is enabled, the user can configure a security profile for each VLAN.

The user defines a security policy by specifying one or more values for the following parameters:

- Wireless STA types (WPA station, 802.11i (WPA2) station, 802.1x station, WEP station, WPA-PSK, and 802.11i-PSK) that can associate to the AP.
- Authentication mechanisms (802.1x, RADIUS MAC authentication) that are used to authenticate clients for each type of station.
- Cipher Suites (CCMP, TKIP, WEP, None) used for encapsulating the wireless data for each type of station.

Up to 16 security profiles can be configured per wireless interface.

NOTE: *Mesh security is configured on the* Mesh (AP-4000M/AP-4900M Only) *tab.*

1. Click **Configure** > **SSID/VLAN/Security** > **Security Profile**.

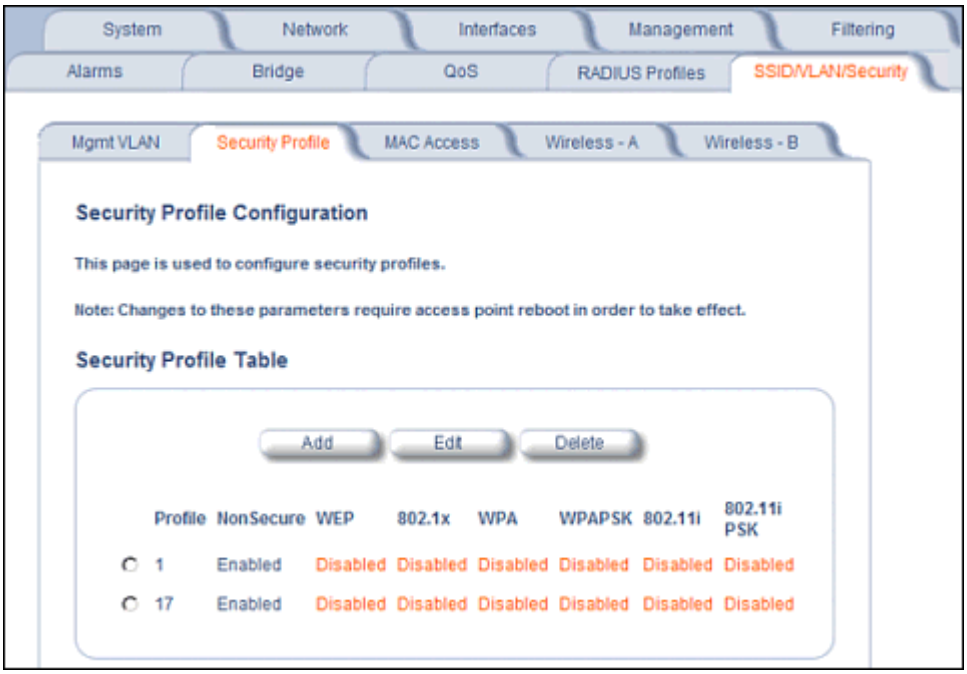


Figure 4-41 Security Profile Configuration

2. Click **Add** in the Security Profile Table to create a new entry. To modify an existing profile, select the profile and click **Edit**. To delete an existing profile, select the profile and click **Delete**. You cannot delete a Security Profile used in an SSID. Also, the first Security Profile cannot be deleted.
3. Configure one or more types of wireless stations (security modes) that are allowed access to the AP under the security profile. The WEP/PSK parameters are separately configurable for each security mode. To enable a security mode in the profile (Non Secure Station, WEP Station, 802.1x Station, WPA Station, WPA-PSK Station, 802.11i (WPA2) Station, 802.11i-PSK Station), check the box next to the mode. See Figure 4-42 on page 122.

   If the security mode selected in a profile is WEP, WPA-PSK, or 802.11i-PSK, then you must configure the WEP or Pre-Shared Keys.

   NOTE: *If an 802.1x client that has already been authenticated attempts to switch to WEP, or if a WEP client that has already been connected attempts to switch to 802.1x, the AP will not allow the client to switch immediately. If this happens, either reboot the AP or disable the client/roam to a new AP for five minutes, and then attempt to reconnect to the AP. If the client is still unable to connect after waiting five minutes, reboot the AP.*

4. Configure the parameters as follows for each enabled security mode. See Figure 4-42 on page 122.
   - **Non Secure Station**:
     - Authentication Mode: None. The AP allows access to Stations without authentication.
       - — Non secure station should be used only with WEP or 802.1x security mode.
     - Cipher: None
   - **WEP Station**:
     - Authentication Mode: None
     - Cipher: WEP
     - Encryption Key 0, Encryption Key 1, Encryption Key 2, Encryption Key 3
     - Encryption Key Length: 64, 128, or 152 Bits.
       - — For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart).
       - — For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
       - — For 152-bit encryption, an encryption key is 32 hexadecimal characters or 16 ASCII characters.
     - Encryption Transmit Key: select Key 0, Key 1, Key 2, or Key 3
   - **802.1x Station**:
     - Authentication Mode: 802.1x
     - Cipher: WEP
     - Encryption Key Length: 64 or 128 Bits.
       - — If 802.1x is enabled simultaneously with WEP, the 802.1x Station's encryption key length is determined by the WEP encryption key.
   - **WPA Station**:
     - Authentication Mode: 802.1x
     - Cipher: TKIP
   - **WPA-PSK Station**:
     - Authentication Mode: PSK
     - Cipher: TKIP
     - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, be used to ensure that the generated key cannot be easily deciphered by network infiltrators.
   - **802.11i Station**:
     - Authentication Mode: 802.1x

    - Cipher: CCMP based on AES
  - **802.11i-PSK Station**:
    - Authentication Mode: PSK
    - Cipher: CCMP based on AES
    - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, to ensure that the generated key cannot be easily deciphered by network infiltrators.
5. When finished configuring all parameters, click **OK**.
6. If you selected a Security Mode of 802.1x Station, WPA Station, or 802.11i Station, you must configure a RADIUS 802.1x/EAP server. See the Configuring Radius Profiles section.

   Security Profile 1 will be used by default for all wireless interfaces.
7. Reboot the AP.

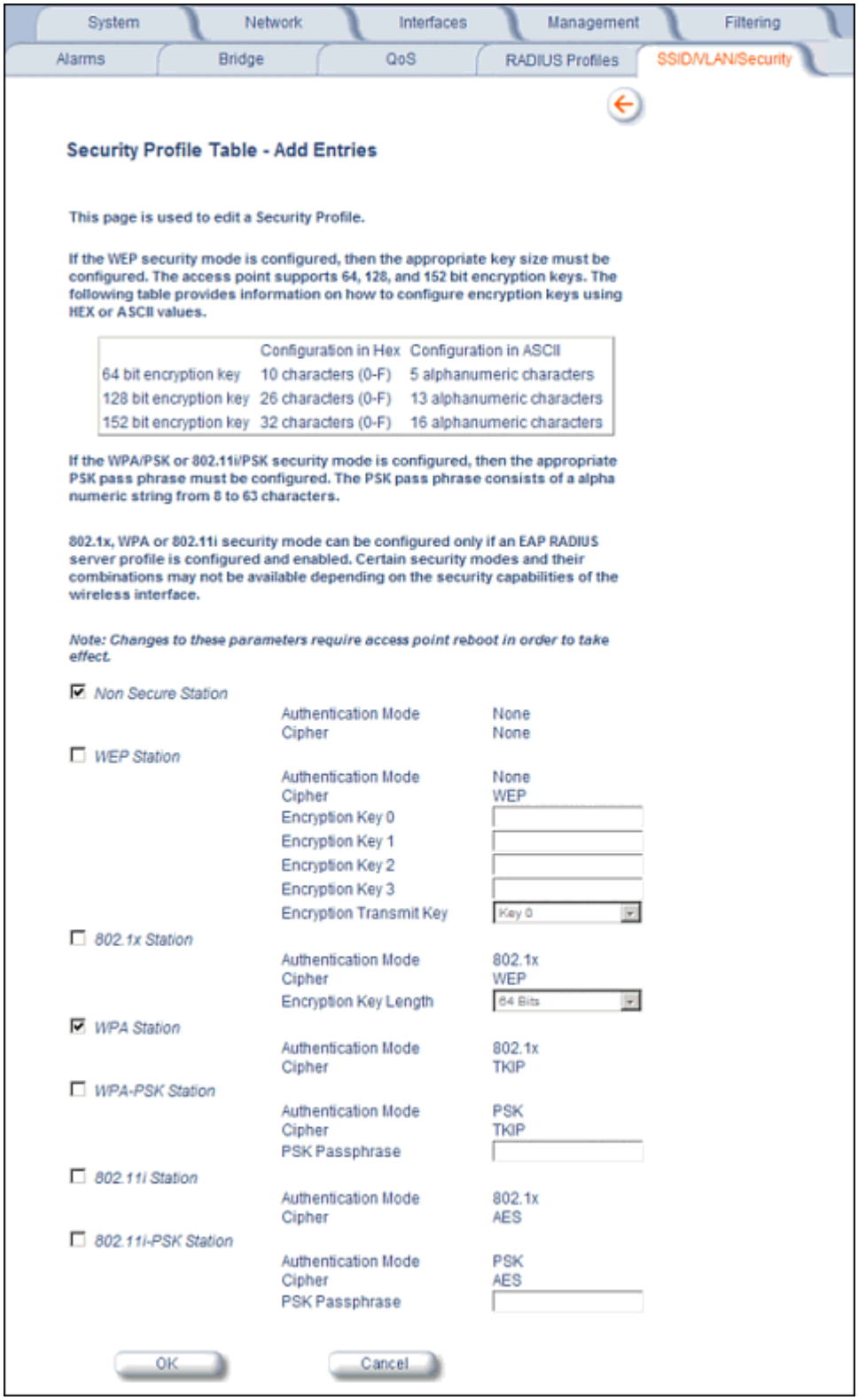


Figure 4-42 Security Profile Table - Add Entries

MAC Access

The MAC Access sub-tab allows you to build a list of stations, identified by their MAC addresses, authorized to access the network through the AP. The list is stored inside each AP within your network. Note that you must reboot the AP for any changes to the MAC Access Control Table to take effect. Up to 1000 entries can be made in the table.

The “MAC ACL Status” parameter (configurable on the SSID/VLAN > Wireless A or B sub-tab) is per VLAN if VLAN Management is enabled. All other parameters besides “MAC ACL Status” are configured per AP, even if VLAN is enabled.

The following list details the configurable MAC Access parameters.

NOTE: *MAC Access Control status is enabled or disabled when configuring each Security Profile.*

- **Operation Type:** Choose between **Passthru** and **Block**. This determines how the stations identified in the MAC Access Control Table are filtered.
  - If set to **Passthru**, only the addresses listed in the Control Table will pass through the bridge.
  - If set to **Block**, the bridge will block traffic to or from the addresses listed in the Control Table.
- **MAC Access Control Table:** Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  – **MAC Address:** Enter the wireless client’s MAC address.
  – **Comment:** Enter an optional comment such as the client’s name.
  – **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field’s value.

NOTE: *For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the* MAC Access Control Via RADIUS Authentication*.*

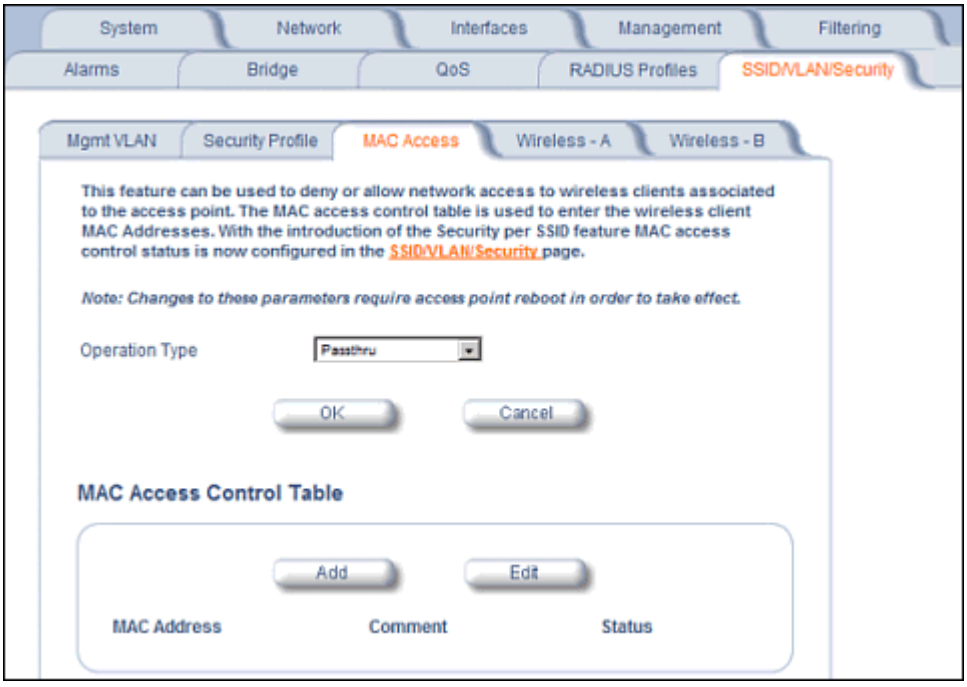


Figure 4-43 MAC Access Configuration Screen

Wireless-A or Wireless-B

Each SSID can have its own Security Profile that defines its security mode, authentication mechanism, and encryption, so that customers can have multiple types of clients (non-WEP, WEP, 802.1x, WPA, WPA-PSK, 802.11i, 802.11i-PSK) on

the same system separated per VLAN. See the Security Profile section for more information. Each SSID can support a unique VLANs. In order for the AP to support multiple SSID/VLANs, VLAN Tagging must be enabled. These parameters are configurable on the **Wireless-A and Wireless-B** sub-tabs.

Configuring an SSID/VLAN with VLAN Tagging Disabled

With VLAN tagging disabled (from the **SSID/VLAN/Security** > **Mgmt VLAN** tab), only one SSID can be configured per interface. All parameters set on the Wireless-A or Wireless-B tab will be applied to that SSID.

1. Click **SSID/VLAN/Security** > **Wireless-A** or **Wireless-B**.
   The **SSID, VLAN, and Security Configuration** page is displayed.

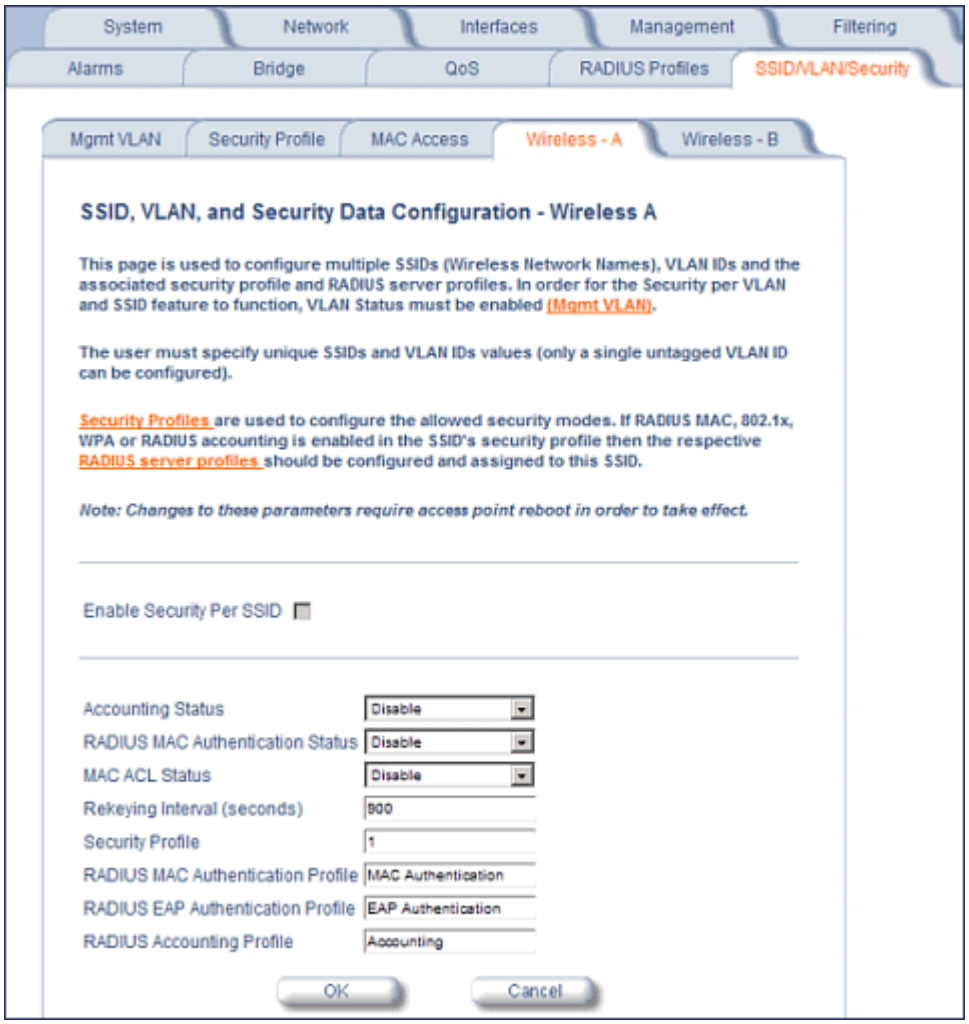


Figure 4-44 SSID, VLAN, and Security Configuration (VLAN Tagging Disabled)

2. Enable or disable RADIUS accounting on the VLAN/SSID by selecting **Enable** or **Disable** from the **Accounting Status** drop-down menu.
3. Enable or disable RADIUS MAC authentication status on the VLAN/SSID by selecting **Enable** or **Disable** from the **RADIUS Authentication Status** drop-down menu.
4. Enable or disable MAC Access Control List status on the VLAN/SSID by selecting **Enable** or **Disable** from the **MAC ACL Status** drop-down menu.
5. Enter **Rekeying Interval** in seconds (between 60 and 65525). The default interval is 900 seconds.

6. Enter the **Security Profile** used by the VLAN in the Security Profile field. See the Security Profile section for more information.
7. Define the **RADIUS Server Profile Configuration** for the VLAN/SSID:
   - RADIUS MAC Authentication Profile
   - RADIUS EAP Authentication Profile
   - RADIUS Accounting Profile

     If 802.1x, WPA, or 802.11i security mode is used, the RADIUS EAP Authentication Profile must have a value.

     A RADIUS Server Profile for authentication for each VLAN shall be configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, “MAC Authentication”, “EAP Authentication”, Accounting”, and “Management”
8. If desired, scroll down to the scroll down to the **SSID and VLAN Table** and click **Edit** to modify the Network Name, VLAN ID, or QoS profile of the SSID/VLAN.

   NOTE: *Because VLAN tagging is disabled, attempting to add a new SSID/VLAN will produce an error message.*

   The **Edit Entries** screen will be displayed. See Figure 4-45.

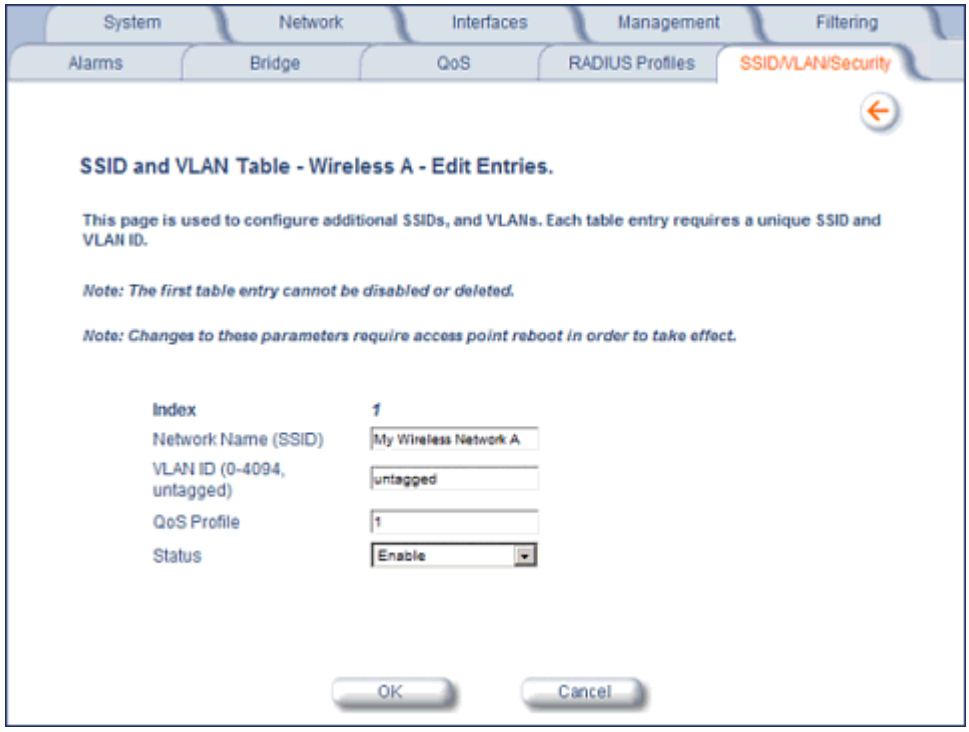


Figure 4-45 SSID/VLAN Edit Entries Screen (VLAN Tagging Disabled)

9. Enter a unique **Network Name** (SSID) between 1 and 32 characters. This parameter is mandatory.

   NOTE: *Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.*

10. Enter a unique **VLAN ID**. This parameter is mandatory.
    - A VLAN ID is a number from -1 to 4094. A value of -1 means that an entry is “untagged.”
    - You can set the VLAN ID to “-1” or “untagged” if you do not want clients that are using a specific SSID to be members of a VLAN workgroup.
    - The VLAN ID must match an ID used by your network; contact your network administrator if you need assistance defining the VLAN IDs.

11. Specify a **QoS profile**. See the Enabling QoS and Adding QoS policies section for more information.
12. If editing an entry, enable or disable the parameters on this page by electing Enable or Disable from the **Status** drop-down menu. If adding a new entry, this drop-down menu will not appear.
13. Click **OK** to return to Wireless-A or Wireless-B Security Configuration Screen.
14. Reboot the AP.

Configuring SSID/VLANs with VLAN Tagging Enabled

With VLAN Tagging enabled (from the **SSID/VLAN/Security** > **Mgmt VLAN** tab), multiple SSID/VLANs are supported. Parameters set on the Wireless-A or Wireless-B tab can be enabled per SSID by choosing the **Enable Security per SSID** option.

1. Click **SSID/VLAN/Security** > **Wireless-A** or **Wireless-B**.
2. Select the **Enable Security Per SSID** option. The screen will update to the following:

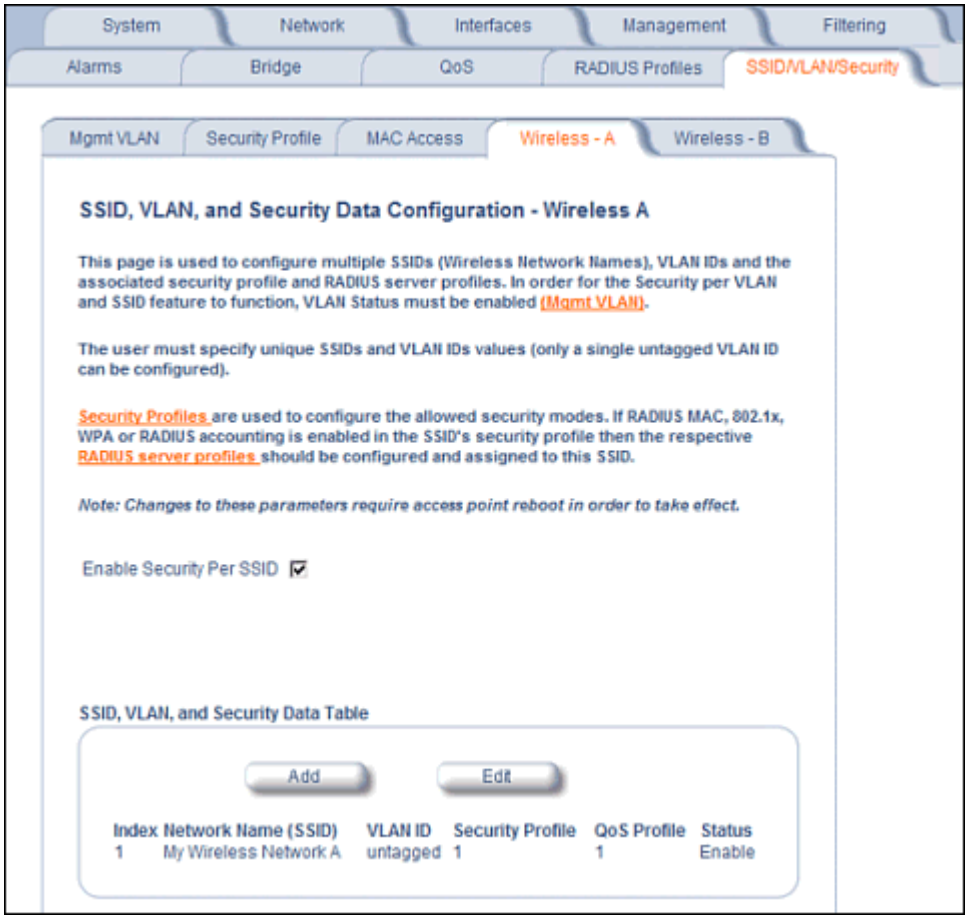


Figure 4-46 SSID/VLAN Configuration (VLAN Tagging Enabled)

NOTE: *If you disable (uncheck) the **Enable Security per SSID** option, you will be able to add multiple SSID/VLANs, but the same configuration parameters (described below) will applied to all of them.*

3. Click **Add** to configure additional SSIDs, VLANs, and their associated security profiles and RADIUS server profiles, or click **Edit** to modify existing SSIDs.

   The **Add Entries** or **Edit Entries** screen appears. See Figure 4-47.

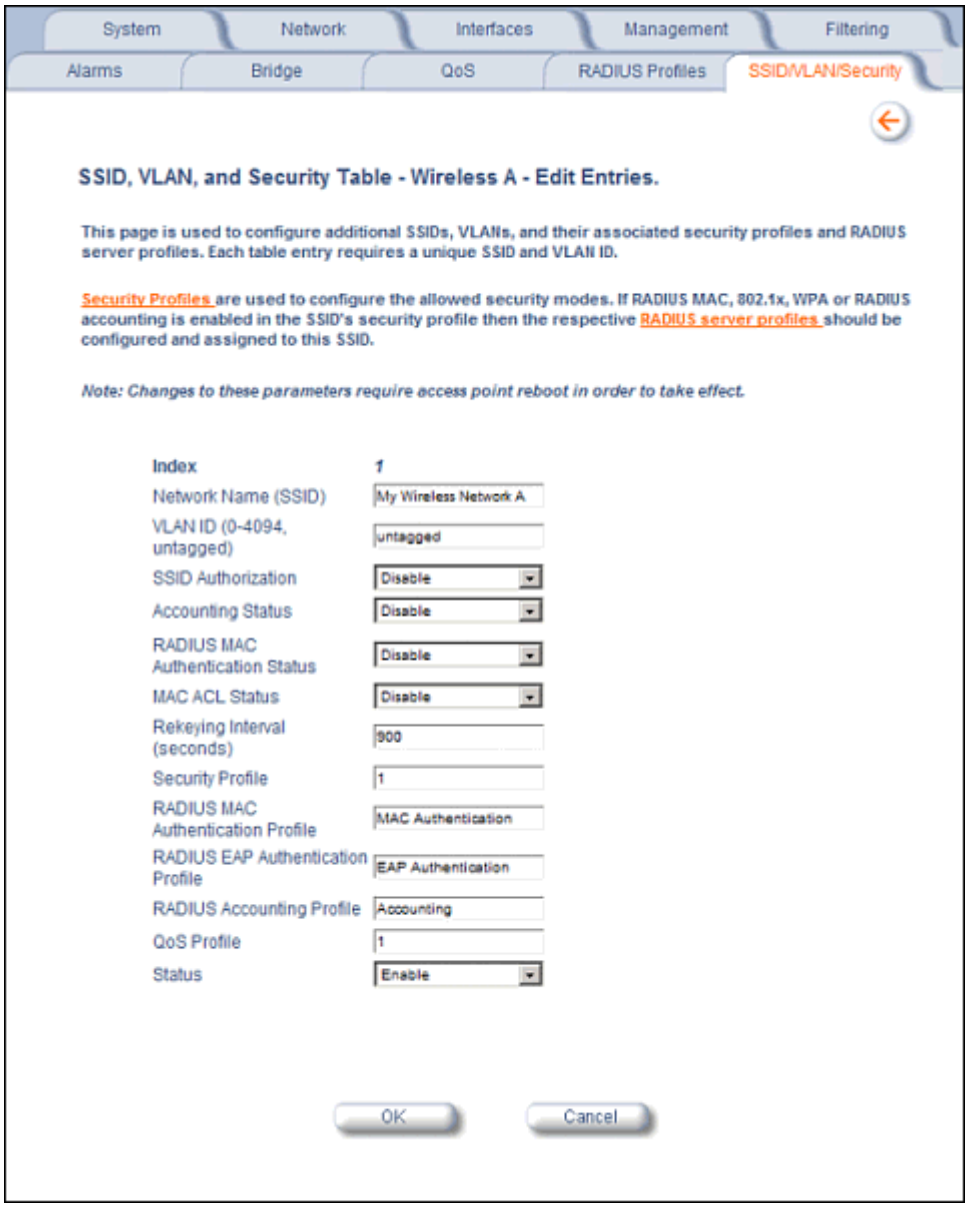


Figure 4-47 SSID/VLAN Edit Entries Screen (VLAN Tagging Enabled)

4. Enter a unique **Network Name** (SSID) between 1 and 32 characters. This parameter is mandatory.

   NOTE: *Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.*

5. Enter a unique **VLAN ID**. This parameter is mandatory.
   - A VLAN ID is a number from -1 to 4094. A value of -1 means that an entry is “untagged.”
   - You can set the VLAN ID to “-1” or “untagged” if you do not want clients that are using a specific SSID to be members of a VLAN workgroup. Only one “untagged” VLAN ID is allowed per interface.
   - The VLAN ID must match an ID used by your network; contact your network administrator if you need assistance defining the VLAN IDs.
6. Enable or disable the **SSID Authorization** status from the drop-down menu. SSID Authorization is the RADIUS-based authorization of the SSID for a particular client. The authorized SSIDs are sent as the tunnel attributes.

7. Enable or disable RADIUS accounting on the VLAN/SSID under the **Accounting Status** drop-down menu.
8. Enable or disable RADIUS MAC authentication status on the VLAN/SSID under the **RADIUS Authentication Status** drop-down menu.
9. Enable or disable MAC Access Control List status on the VLAN/SSID under the **MAC ACL Status** drop-down menu.
10. Enter the **Rekeying Interval** in seconds. The default interval is 900 seconds.
11. Enter the Security Profile used by the VLAN in the **Security Profile** field.

    NOTE: *If you have two or more SSIDs per interface using a Security Profile with a security mode of Non Secure, be aware that security being applied in the VLAN is not being applied in the wireless network.*

12. Define the **RADIUS Server Profile Configuration** for the VLAN/SSID:
    - RADIUS MAC Authentication Profile
    - RADIUS EAP Authentication Profile
    - RADIUS Accounting Profile

    If 802.1x, WPA, or 802.11i security mode is used, the RADIUS EAP Authentication Profile must have a value.

    A RADIUS Server Profile for authentication for each VLAN shall be configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, “MAC Authentication”, “EAP Authentication”, Accounting”, and “Management”.
13. Specify a **QoS Profile**. See the Enabling QoS and Adding QoS policies section for more information.
14. If editing an entry, enable or disable the parameters on this page using **Status** drop-down menu. If adding a new entry, this drop-down menu will not appear.
15. Reboot the AP.

Broadcast SSID and Closed System

Broadcast SSID allows the broadcast of a single SSID when the AP is configured for multiple SSIDs. Broadcast SSID may only be enabled for a single SSID. This object can only be configured using the CLI and SNMP using a MIB browser or network management application.

Closed System manages the way probe requests are handled. If enabled, the AP will respond to probe requests with an SSID only if the client has specified the SSID in the probe request. If the client sends a probe request with a null or “ANY” SSID, the AP will respond with a null SSID. If disabled, the AP will respond with each configured SSID, whether or not an SSID has been specified in the probe request. This option is disabled by default.

For more information, on Broadcast SSID and Closed System, see Knoweldgebase Answer ID 1698 at http://support.proxim.com.

5 Monitoring

This chapter discusses the following monitoring options:

- Version: Provides version information for the Access Point's system components.
- ICMP: Displays statistics for Internet Control Message Protocol packets sent and received by the AP.
- IP/ARP Table: Displays the AP's IP Address Resolution table.
- Learn Table: Displays the list of nodes that the AP has learned are on the network.
- IAPP: Provides statistics for the Inter-Access Point Protocol messages sent and received by the AP.
- RADIUS: Provides statistics for the configured RADIUS server(s).
- Interfaces: Displays the Access Point's interface statistics (Wireless and Ethernet).
- Station Statistics: Displays statistics for stations and Wireless Distribution System links.
- Mesh Statistics: Displays statistics for the Mesh portal, including the network topology and the Neighbor Table.

To monitor the AP using the HTTP/HTTPS interface, you must first log in to a web browser. See Logging In for instructions.

You may also monitor the AP using the command line interface. See Command Line Interface (CLI) for more information

To monitor the AP via HTTP/HTTPS:

1. Click the **Monitor** button located on the left-hand side of the screen. The main **Monitor** screen will be displayed.

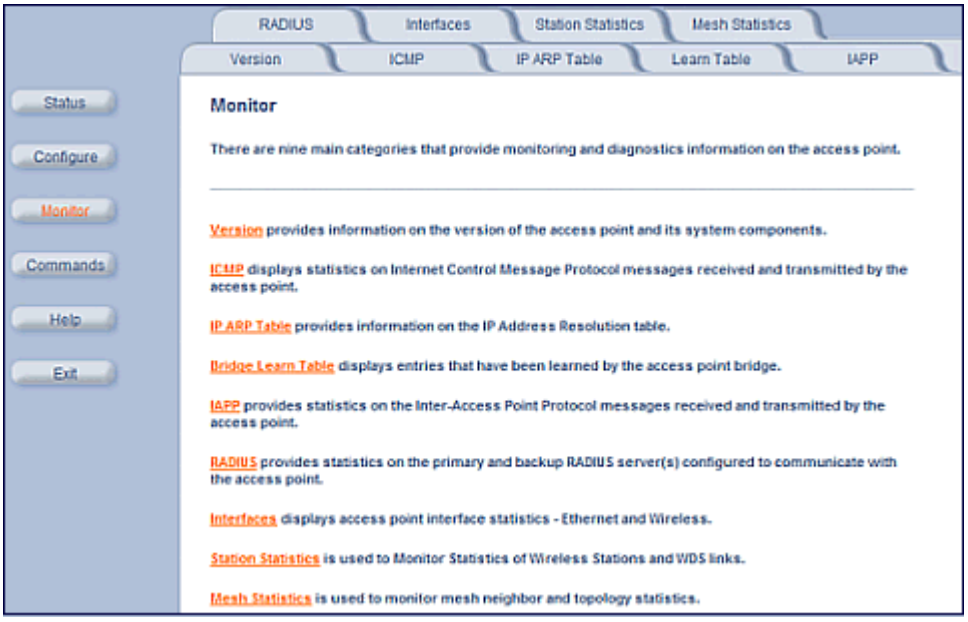


Figure 5-1 Monitor Main Screen

2. Click the tab that corresponds to the statistics you want to review. For example, click **Learn Table** to see the list of nodes that the AP has discovered on the network.
3. If necessary, click the **Refresh** button to update the statistics.

Each **Monitor** tab is described in the remainder of this chapter.

Version

From the HTTP interface, click the **Monitor** button and select the **Version** tab. The list displayed provides you with information that may be pertinent when calling Technical Support. With this information, your Technical Support representative can verify compatibility issues and make sure the latest software are loaded. This screen displays the following information for each Access Point component:

- **Serial Number:** The component's serial number, if applicable.
- **Component Name ID:** The AP identifies a system component based on its ID. Each component has a unique identifier.
- **Variant:** Several variants may exist of the same component (for example, a hardware component may have two variants, one with more memory than the other).
- **Version:** Specifies the component's version or build number. The Software Image version is the most useful information on this screen for the typical end user.

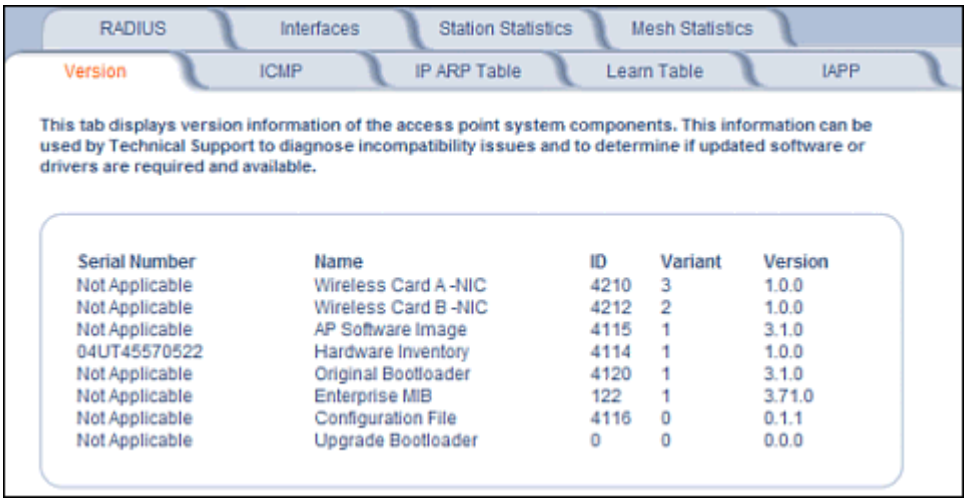


Figure 5-2 Version Monitoring Tab

ICMP

This tab provides statistical information for both received and transmitted messages directed to the AP. Not all ICMP traffic on the network is counted in the ICMP (Internet Control Message Protocol) statistics.

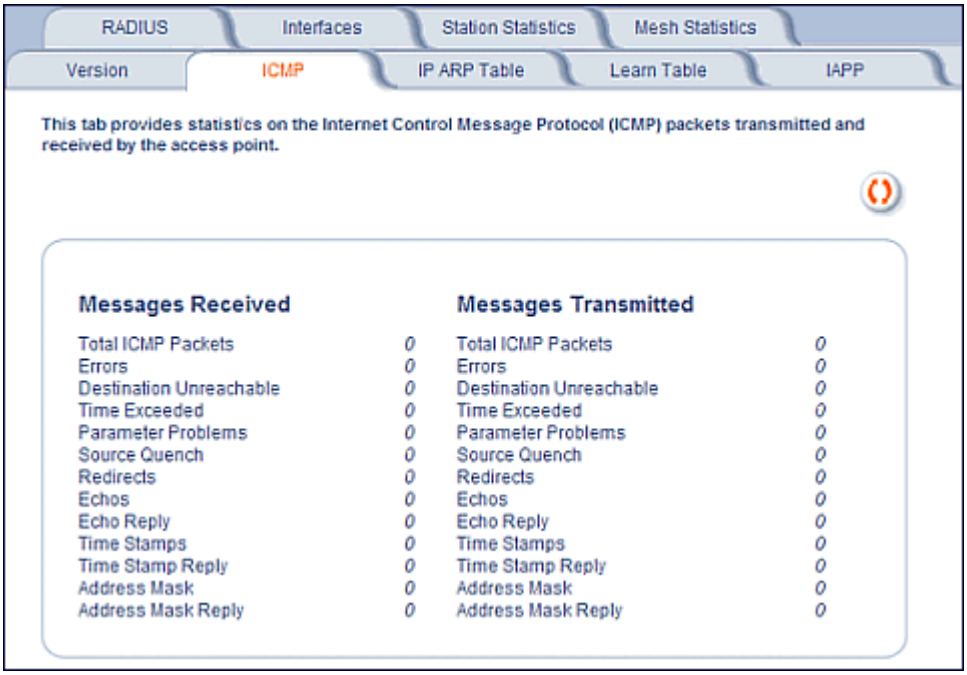


Figure 5-3 ICMP Monitoring Tab

IP/ARP Table

This tab provides information based on the Address Resolution Protocol (ARP), which relates MAC Address and IP Addresses.

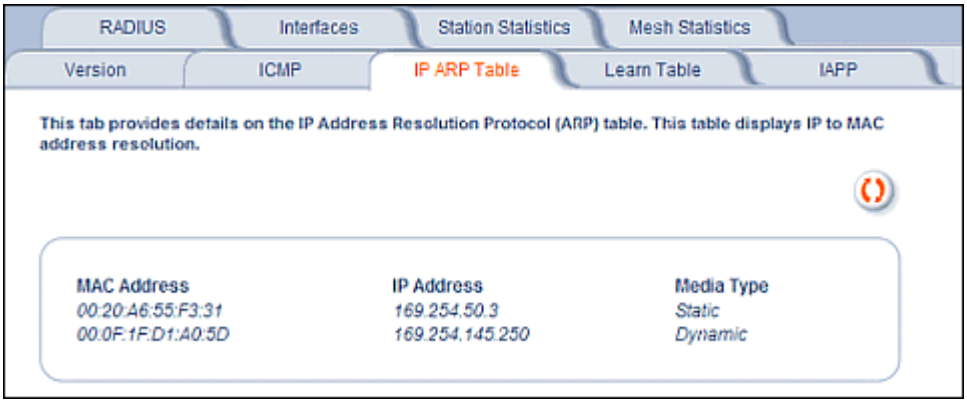


Figure 5-4 IP/ARP Table Monitoring Tab

Learn Table

This tab displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up 10,000 entries in the Learn Table.

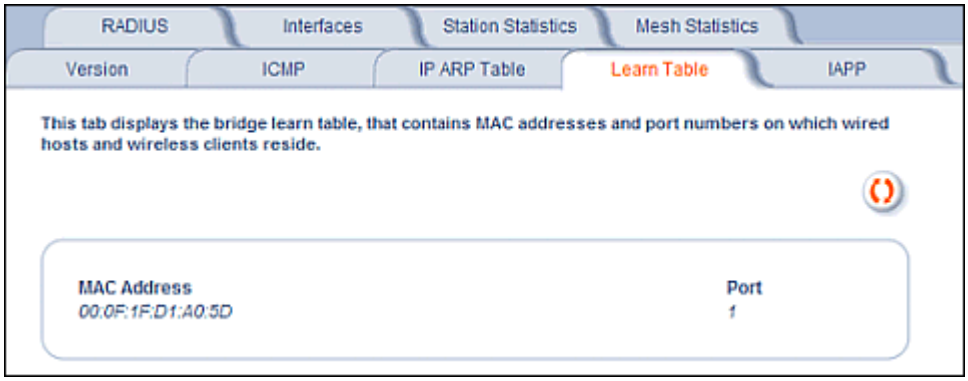


Figure 5-5 Learn Table Monitoring Tab

IAPP

This tab displays statistics relating to client handovers and communications between ORiNOCO Access Points.

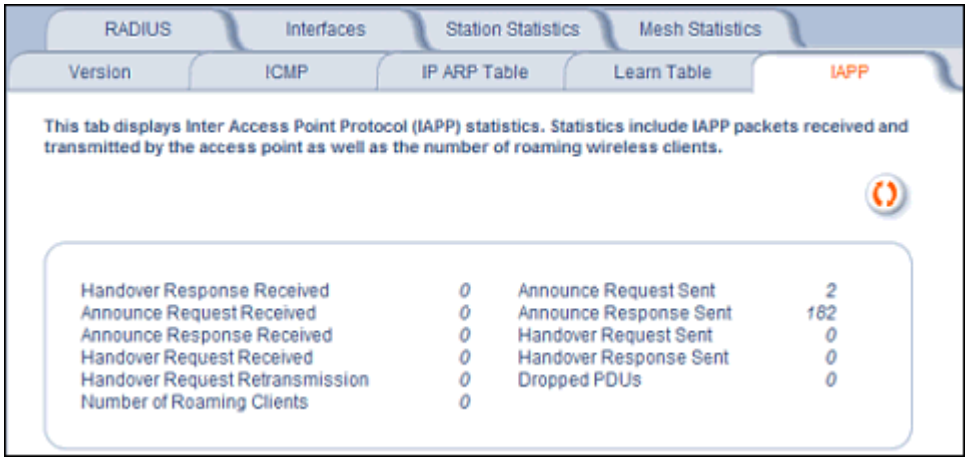


Figure 5-6 IAPP Monitoring Tab

RADIUS

This tab provides RADIUS authentication, EAP/802.1x authentication, and accounting information for both the Primary and Backup RADIUS servers for each RADIUS Server Profile.

NOTE: *Separate RADIUS servers can be configured for each RADIUS Server Profile.*

Select the RADIUS Server Profile to view statistics on from the **Select Server Profile** drop-down menu.

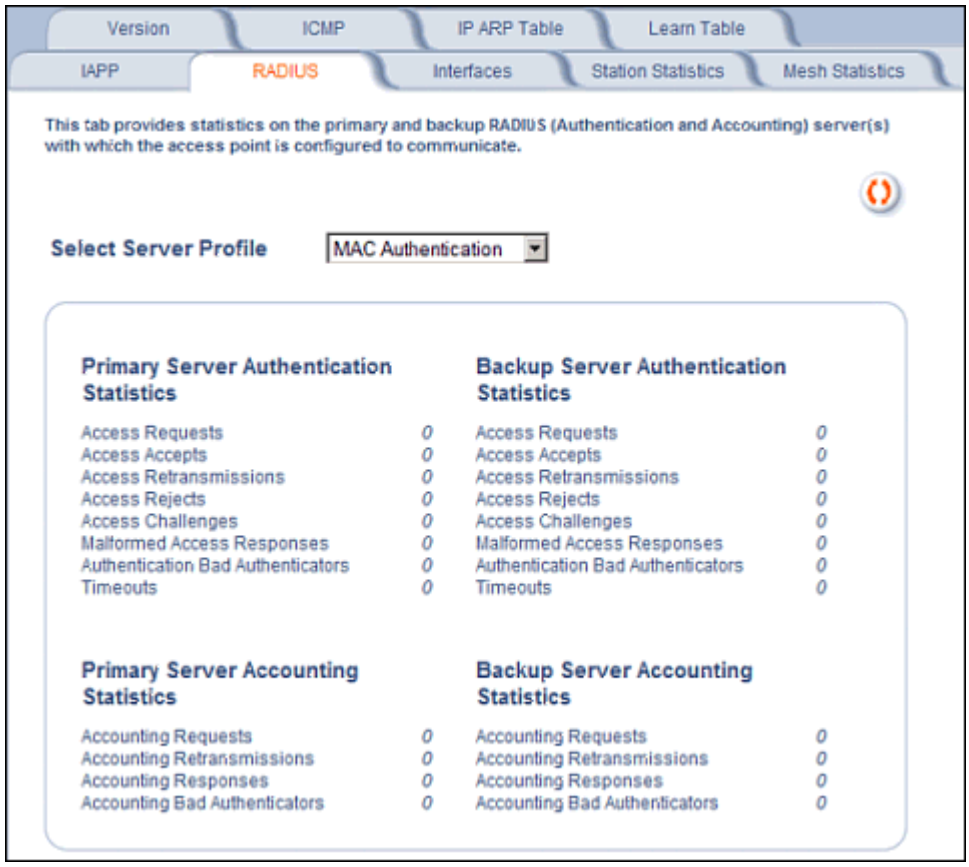


Figure 5-7 RADIUS Monitoring Tab

Interfaces

This tab displays statistics for the Ethernet and wireless interfaces.

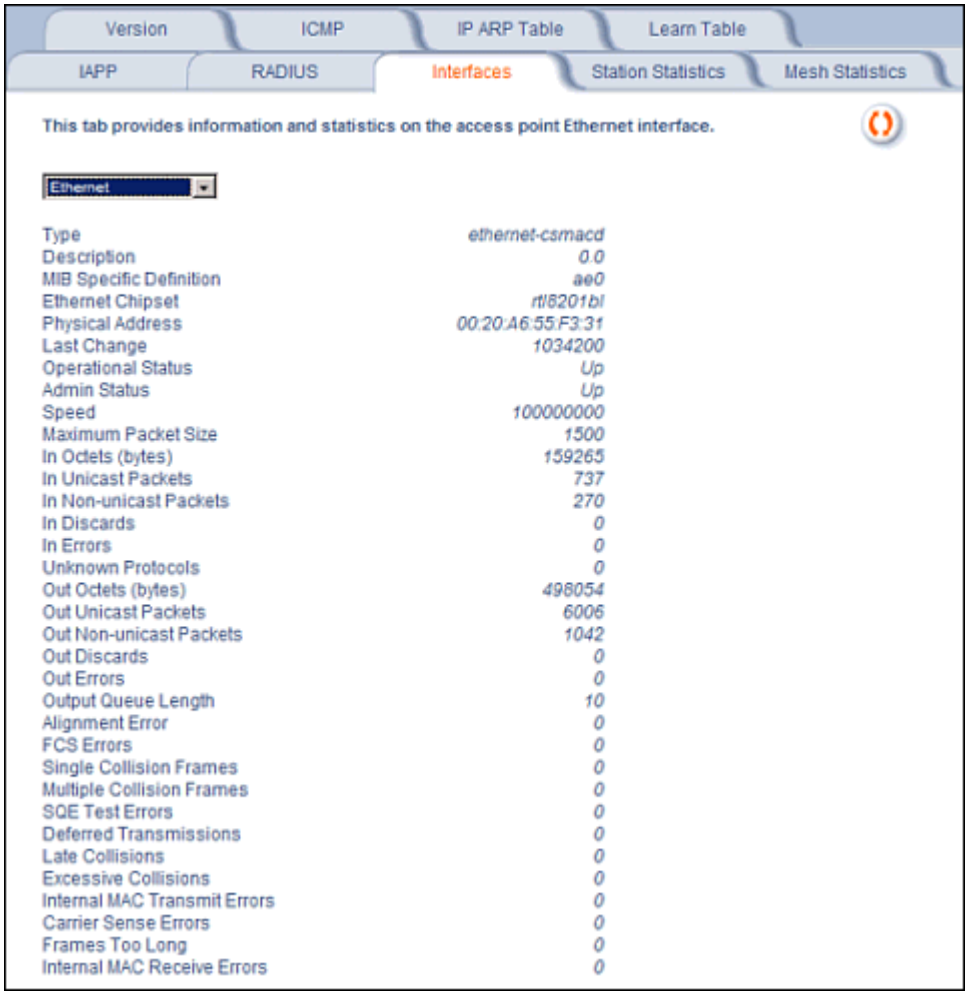


Figure 5-8 Interface Monitoring Tab (Ethernet)

Description of Interface Statistics

The following statistics are displayed for the Ethernet interface only, either of the wireless interfaces only, or for all interfaces:

- **Admin Status** (*Ethernet/Wireless-Slot A/B*): The desired state of the interface: Up (ready to pass packets), Down (not ready to pass packets, or Testing (testing and unable to pass packets).
- **Alignment Error** *(Ethernet)*: The number of frames received that are not an integral number of octets in length and do not pass the Frame Check Sequence check.
- **Carrier Sense Errors** *(Ethernet)*: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame. The count increments at most once per transmission attempt.
- **Deferred Transmission** *(Ethernet)*: The number of frames for which the first transmission attempt is delayed because the medium is busy.This number does not include frames involved in collisions.
- **Description** *(Ethernet/Wireless-Slot A/B)*: Information about the interface (e.g., the name of the manufacturer, the product name and the version of the hardware interface).
- **Duplicate Frame Count** *(Wireless-Slot A/B)*: The number of duplicate frames received.

- **Ethernet Chipset** *(Ethernet)*: Identifies the chipset used to realize the interface.
- **Excessive Collisions** *(Ethernet)*: The number of frames for which transmission fails due to excessive collisions.
- **Failed ACK Count** *(Wireless-Slot A/B)*: The number of of times an acknowledgment (or ACK) is not received when expected.
- **Failed Count** *(Wireless-Slot A/B)*: The number of packets not transmitted successfully due to too many transmit attempts.
- **Failed RTS Count** *(Wireless-Slot A/B)*: The number of times a Clear to Send (CTS) is not received in response to a Request to Send (RTS).
- **FCS Error** *(Wireless-Slot A/B)*: The number of Frame Check Sequence errors detected in received MAC Protocol Data Units (MPDUs).
- **FCS Errors** *(Ethernet)*: The number of frames received that are an integral number of octets in length but do not pass the Frame Check Sequence check.
- **Frames Too Long** *(Ethernet)*: The number of frames received that exceed the maximum permitted frame size.
- **In Discards** *(Ethernet/Wireless-Slot A/B)*: The number of error-free inbound packets that were chosen to be discarded to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **In Errors** *(Ethernet/Wireless-Slot A/B)*: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **In Non-unicast Packets** *(Ethernet/Wireless-Slot A/B)*: The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
- **In Octets (bytes)** *(Ethernet/Wireless-Slot A/B)*: The total number of octets received on the interface, including framing characters.
- **In Unicast Packets** *(Ethernet/Wireless-Slot A/B)*: The number of subnetwork unicast packets delivered to a higher-layer protocol.
- **Internal MAC Recieve Errors** *(Ethernet)*: The number of frames for which reception fails due to an internal MAC sublayer transmit error. A frame is only counted if it is not counted by the Frames Too Long, Alignment Error, or FCS Error counters.
- **Internal MAC Transmit Errors** *(Ethernet)*: The number of frames for which transmission fails due to an internal MAC sublayer transmit error. A frame is only counted if it is not counted by Late Collission, Excession Collision, or Carrier Sense Error counters.
- **Last Change** *(Ethernet/Wireless-Slot A/B)*:The value of the sysUpTime object at the time the interface entered its current operational state.
- **Late Collisions** *(Ethernet)*: The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet
- **MAC Address** *(Wireless-Slot A/B)*: The station's assigned, unique MAC address,
- **Maximum Packet Size** *(Ethernet/Wireless-Slot A/B)*: The size (in octets) of the largest datagram which can be sent/received
- **MIB Specific Definition** *(Ethernet/Wireless-Slot A/B)*: A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is an Ethernet interface, then this field refers to a document defining objects specific to ethernet.
- **Multicast Received Frame Count** *(Wireless-Slot A/B)*: The number of multicast packets received.
- **Multicast Transmitted Frame Count** *(Wireless-Slot A/B)*: The number of multicast packets transmitted.
- **Multiple Collision Frames** *(Ethernet)*: The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
- **Multiple Retry Count** *(Wireless-Slot A/B)*: The number of packets successfully transmitted after more than one retransmission.
- **Operational Status** *(Ethernet/Wireless-Slot A/B)*: The current state of the interface: Up (ready to pass packets), Down (not ready to pass packets, or Testing (testing and unable to pass packets).

- **Out Discards** *(Ethernet/Wireless-Slot A/B)*: The number of error-free outbound packets chosen to be discarded to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- **Out Errors** *(Ethernet/Wireless-Slot A/B)*: The number of outbound packets that could not be transmitted because of errors.
- **Out Non-unicast Packets** *(Ethernet/Wireless-Slot A/B)*: The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast orsubnetwork-multicast) address, including those that were discarded or not sent.
- **Out Octets (bytes)** *(Ethernet/Wireless-Slot A/B)*: The total number of octets transmitted out of the interface, including framing characters.
- **Out Unicast Packets** *(Ethernet/Wireless-Slot A/B)*:The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Output Queue Length** *(Ethernet/Wireless-Slot A/B)*: The length of the output packet queue (in packets).
- **Physical Address** *(Ethernet):* The interface's address at the protocol layer immediately below the network layer in the protocol stack.
- **Received Fragment Count** *(Wireless-Slot A/B)*: The number of successfully received Data or Management MAC Protocol Data Units (MPDUs).
- **Retry Count** *(Wireless-Slot A/B)*: The number of packets successfully transmitted after one or more retransmissions.
- **Single Collision Frames** *(Ethernet)*: The number of successfully transmitted frames for which transmission is inhibited by exactly one collision
- **Speed** *(Ethernet/Wireless-Slot A/B)*: An estimate of the interface's current bandwidth in bits per second.
- **SQE Test Errors** *(Ethernet)*:The number of times that the Signal Quality Error (SQE) Test Error message is generated by the physical layer signalling (PLS) sublayer.
- **Successful RTS Count** *(Wireless*-Slot A/B*)*: The number of times a Clear to Send (CTS) is received in response to an Request to Send (RTS).
- **Transmitted Fragment Count** *(Wireless-Slot A/B)*: The number of trasnmitted fragmented packets.
- **Transmitted Frame Count** *(Wireless-Slot A/B)*: This number of successfully transmitted packets.
- **Type** *(Ethernet/Wireless-Slot A/B)*: The type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.
- **Unknown Protocols** *(Ethernet/Wireless-Slot A/B)*: The number of packets received that were discarded because of an unknown or unsupported protocol.
- **WEP Undecryptable Count** *(Wireless-Slot A/B)*: The number of undecryptable WEP frames received.

Station Statistics

This tab displays information on wireless clients attached to the AP and on Wireless Distribution System links.

Enable the Monitoring Station Statistics feature (Station Statistics are disabled by default) by checking **Enable Monitoring Station Statistics** and click **OK**.

You do not need to reboot the AP for the changes to take effect. If clients are connected to the device or WDS links are configured for the device, the statistics will now be shown on the screen.

Click on the **Refresh** button in the browser window to view the latest statistics. If any new clients associate to the AP, you can see the statistics of the new clients after you click the refresh button.

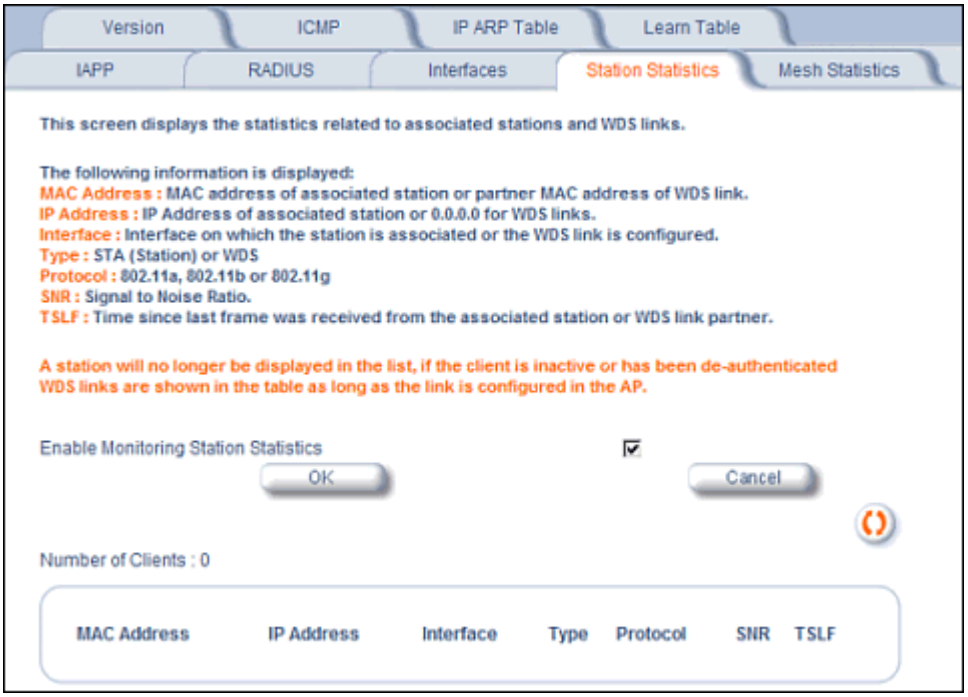


Figure 5-9 Station Statistics Monitoring Tab

Description of Station Statistics

The following stations statistics are displayed:

- **MAC Address**: The MAC address of the wireless client for which the statistics are gathered. For WDS links, this is the partner MAC address of the link.
- **IP Address**: The IP address of the associated wireless station for which the Statistics are gathered. (0.0.0.0 for WDS links)
- **Interface to which the Station is connected**: The interface number on which the client is connected with the AP. For WDS links this is the interface on which the link is configured.
- **Station Type**: The type of wireless client (STA or WDS).
- **MAC Protocol**: The MAC protocol for this wireless client (or WDS link partner). The possible values are 802.11a, 802.11b, 802.11g
- **Signal / Noise**: The Signal /Noise Level measured at the AP when frames are received from the associated wireless station (or WDS link partner)
- **Time since Last Packet Received**: The time elapsed since the last frame from the associated wireless station (or WDS link partner) was received.
- **Number of Clients**: The number of stations and WDS links monitored.

The following stations statistics are available through SNMP:

- **Octets Received**: The number of octets received from the associated wireless station (or WDS link partner) by the AP.
- **Unicast Frames Received**: The number of Unicast frames received from the associated wireless station (or WDS link partner) by the AP.
- **Non-Unicast Frames Received**: The number of Non-Unicast frames received (i.e. broadcast or multicast) from the associated wireless station (or WDS link partner) by the AP.
- **Octets Transmitted**: The number of octets sent to the associated wireless station (or WDS link partner) from the AP.
- **Unicast Frames Transmitted**: The number of Unicast frames transmitted to the associated wireless station (or WDS link partner) from the AP.

Mesh Statistics

This tab displays statistics relating to the Mesh portal: the network topology or the Neighbor Table. Selecting **Network Topology** displays a tree structure representing the Mesh network. Selecting **Neighbor Table** (shown below) displays the MAC address, channel, path cost, number of hops, RSSI, type, and status of all Mesh APs within range of the AP.

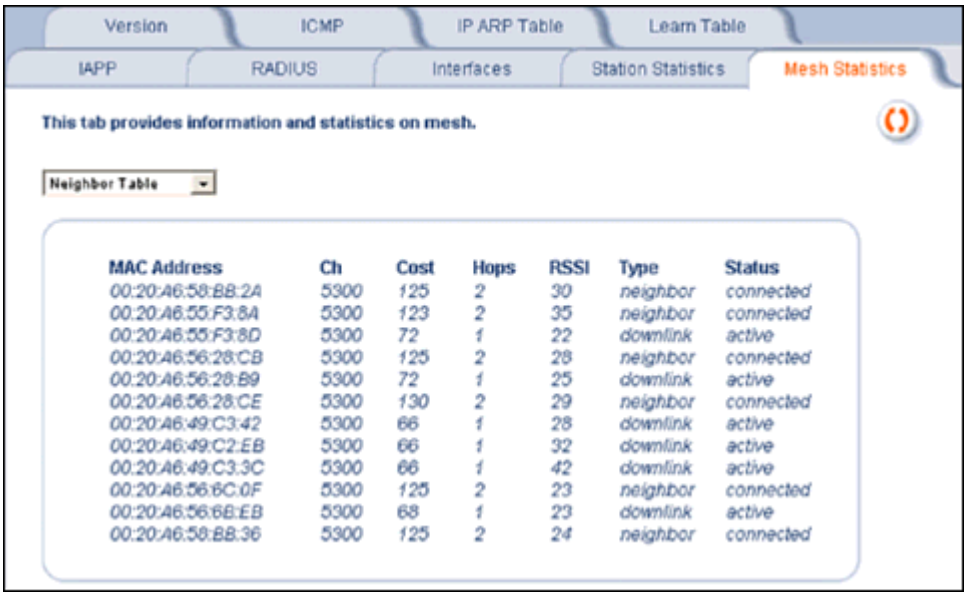


Figure 5-10 Mesh Statistics Monitoring Tab (Neighbor Table)

6 Commands

This chapter contains information on the following Command functions:

- Introduction to File Transfer via TFTP or HTTP: Describes the available file transfer methods.
- Update AP via TFTP: Download files from a TFTP server to the AP.
- Update AP via HTTP: Download files to the AP from HTTP.
- Retrieve File: Upload configuration files from the AP to a TFTP server.
- Retrieve File via HTTP: Upload configuration files from the AP via HTTP.
- Reboot: Reboot the AP in the specified number of seconds.
- Reset: Reset all of the Access Point's configuration settings to factory defaults.
- Help Link: Configure the location where the AP Help files can be found.

To perform commands using the HTTP/HTTPS interface, you must first log in to a web browser. See Related Topics for instructions.

You may also perform commands using the command line interface. See Command Line Interface (CLI) for more information.

To perform commands via HTTP/HTTPS:

1. Click the **Commands** button located on the left-hand side of the screen.

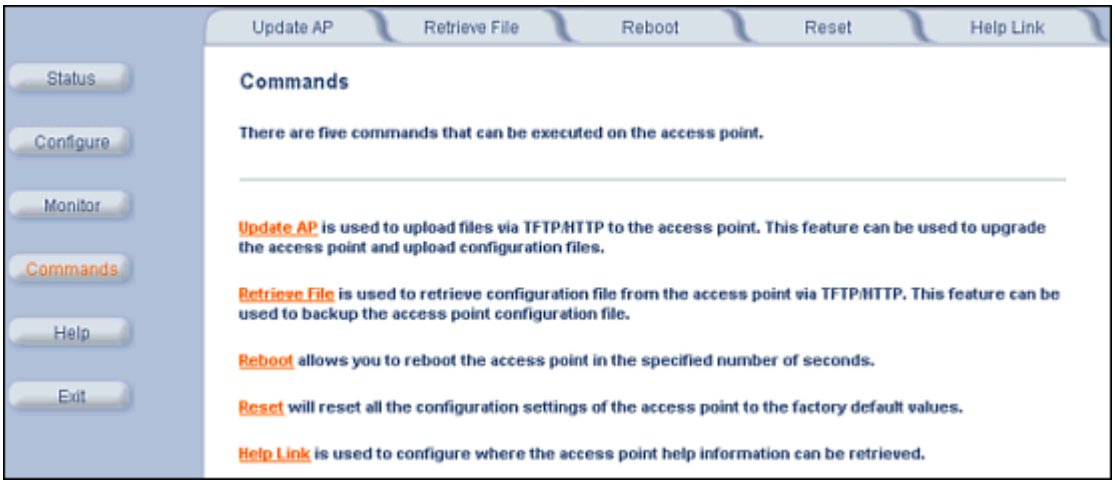


Figure 6-1 Commands Main Screen

2. Click the tab that corresponds to the command you want to issue. For example, click **Reboot** to restart the unit.

Following a brief introduction to TFTP and HTTP file transfer, each **Commands** tab is described in the remainder of this chapter.

Introduction to File Transfer via TFTP or HTTP

There are two methods of transferring files to or from the AP: TFTP or HTTP (or HTTPS if enabled):

- Downloading files (Configuration, AP Image, Bootloader, License, Private Key, Certificate, CLI Batch File) to the AP using one of these two methods is called "Updating the AP."

- Uploading files (Configuration, CLI Batch File) from the AP is called “Retrieving Files.”

TFTP File Transfer Guidelines

A TFTP server must be running and configured to point to the directory containing the file.

If you do not have a TFTP server installed on your system, install the TFTP server from the ORiNOCO CD.

HTTP File Transfer Guidelines

HTTP file transfer can be performed either with or without SSL enabled.

HTTP file transfers with SSL require enabling Secure Management and Secure Socket Layer. HTTP transfers that use SSL may take additional time.

NOTE: *SSL requires Internet Explorer version 6, 128 bit encryption, Service Pack 1, and patch Q323308.*

Image Error Checking During File Transfer

The Access Point performs checks to verify that an image downloaded through HTTP or TFTP is valid. The following checks are performed on the downloaded image:

- Zero Image size
- Large image size
- Non VxWorks image
- AP image
- Digital signature verification

If any of the above checks fail on the downloaded image, the Access Point deletes the downloaded image and retains the old image. Otherwise, if all checks pass successfully, the AP deletes the old image and retains the downloaded image.

These checks are to ensure that the AP does not enter an invalid image state. The storage of the two images is only temporary to ensure the proper verification; the two images will not be stored in the AP permanently.

Image error checking functions automatically in the background. No user configuration is required.

Update AP

Update AP via TFTP

Use the Update AP via TFTP tab to download Configuration, AP Image, License file, Bootloader files, Certificate and Private Key files, and CLI Batch File to the AP. A TFTP server must be running and configured to point to the directory containing the file.

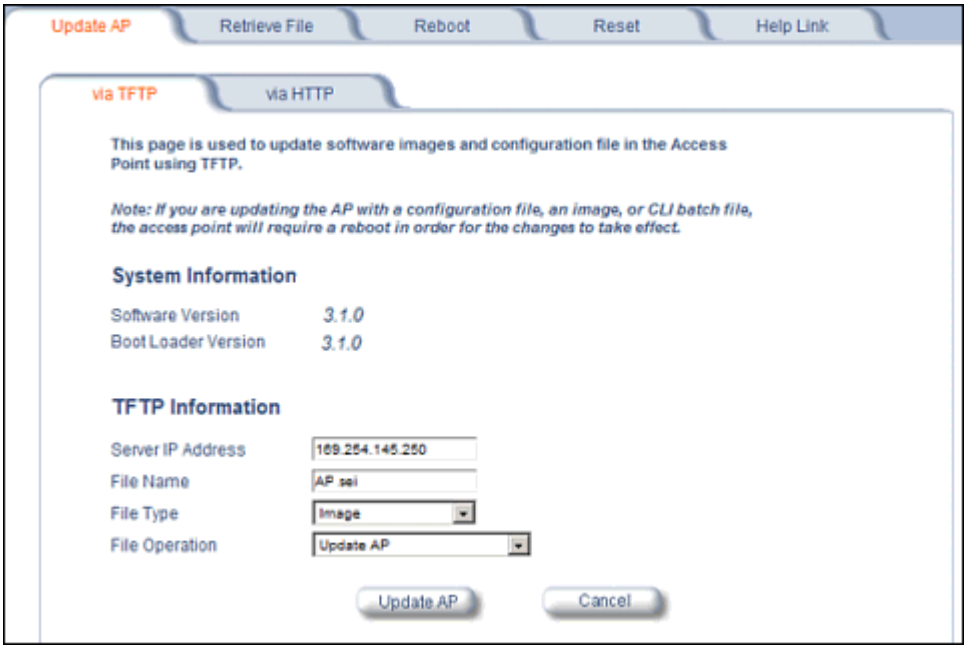


Figure 6-2 Update AP via TFTP Command Screen

If you do not have a TFTP server installed on your system, install the TFTP server from the ORiNOCO CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds* sub-directory.

The **Update AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.
  - Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.

    NOTE: *This is the IP address that will be used to point the Access Point to the AP Image file.*
- **File Name:** Enter the name of the file to be downloaded (including the file extension).
  - Copy the file to the TFTP server's root folder. The default AP Image is located at *C:/Program Files/ORiNOCO/AP4x00/*.
- **File Type:** Select the proper file type. Choices include:
  - **Config**: configuration information, such as System Name, Contact Name, and so on.
  - **Image**: AP Image (executable program).
  - **Upgrade BspBI**: Bootloader software.
  - **License File**: the license key to allow conversion of an AP-4000 unit to an AP-4000M unit.
  - **SSL Certificate**: the digital certificate for authentication in SSL communications.
  - **SSL Private Key**: the private key for encryption in SSL communications.
  - **SSH Public Key**: the public key in SSH communications. See Secure Shell (SSH) Settings for more information.

  - **SSH Private Key**: the private key in SSH communications. See Secure Shell (SSH) Settings for more information.
  - **CLI Batch File**: a CLI Batch file that contains CLI commands to configure the AP. This file will be executed by the AP immediately after being uploaded. See CLI Batch File for more information.
- **File Operation:** Select either **Update AP** or **Update AP & Reboot**. You should reboot the AP after downloading files.

Update AP via HTTP

Use the **Update AP via HTTP** tab to download Configuration, AP Image, Bootloader files, and Certificate and Private Key files to the AP.

Once on the Update AP screen, click on the **via HTTP** tab.

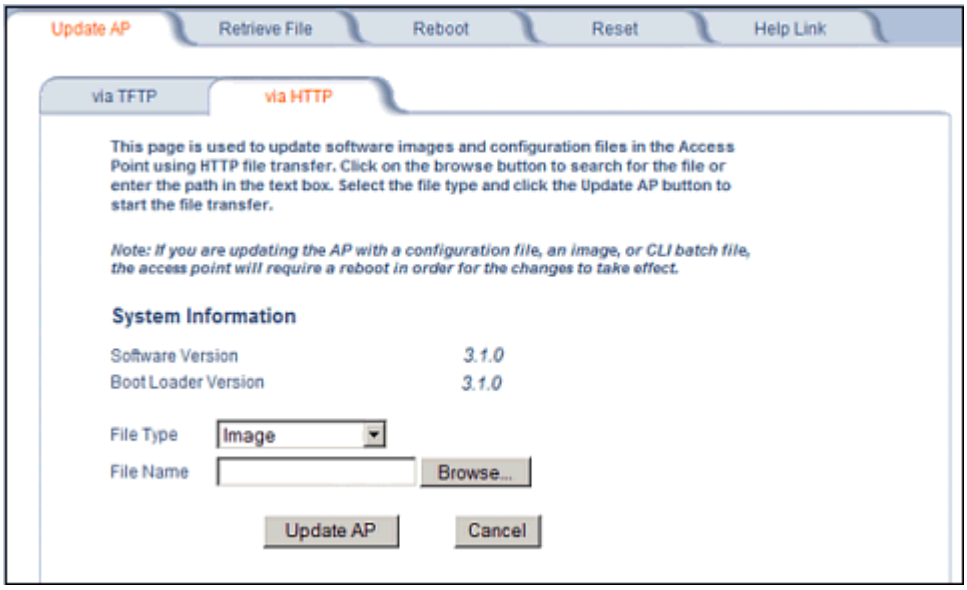


Figure 6-3 Update AP via HTTP Command Screen

The **Update AP via HTTP** tab shows version information and allows you to enter HTTP information as described below.

1. Select the File Type that needs to be updated from the drop-down box. Choices include:
   - Image for the AP Image (executable program).
   - **Config** for configuration information, such as System Name, Contact Name, and so on.
   - **SSL Certificate**: the digital certificate for authentication in SSL communications.
   - **SSL Private Key**: the private key for encryption in SSL communications.
   - **Upgrade BSPBL**: the Bootloader software.
   - **CLI Batch File**: a CLI Batch file that contains CLI commands to configure the AP. This file will be executed by the AP immediately after being uploaded. See CLI Batch File for more information.
   - **SSH Public Key**: the public key in SSH communications. See Secure Shell (SSH) Settings for more information.
   - **SSH Private Key**: the private key in SSH communications. See Secure Shell (SSH) Settings for more information.
   - **License File**: the license key to allow conversion of an AP-4000 unit to an AP-4000M unit.
2. Use the **Browse** button or manually type in the name of the file to be downloaded (including the file extension) in the File Name field. If typing the file name, you must include the full path and the file extension in the file name text box.
3. To initiate the HTTP Update operation, click the **Update AP** button.

A warning message gets displayed that advises the user that a reboot of the device will be required for changes to take effect.

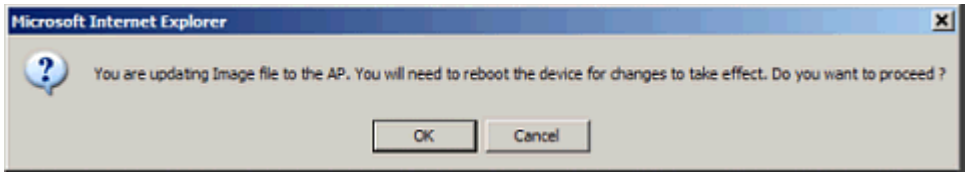


Figure 6-4 Warning Message

4. Click **OK** to continue with the operation or Cancel to abort the operation.

NOTE: *An HTTP file transfer using SSL may take extra time.*

If the operation completes successfully the following screen appears.

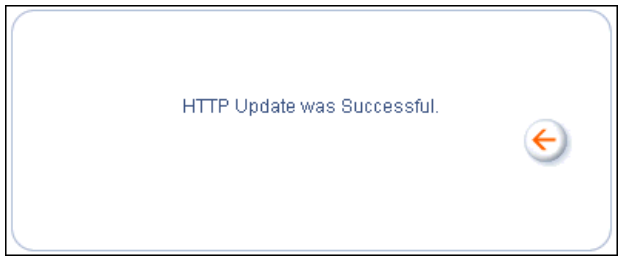


Figure 6-5 Update AP Successful

If the operation did not complete successfully the following screen appears, and the reason for the failure is displayed.

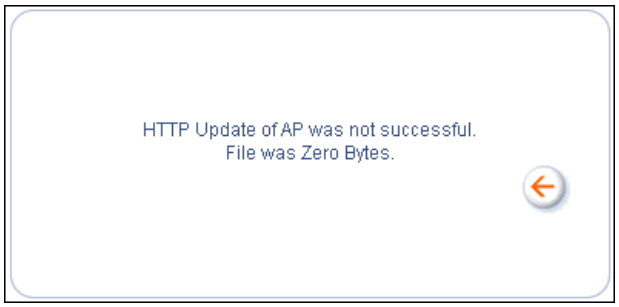


Figure 6-6 Update AP Unsuccessful

Retrieve File

Retrieve File via TFTP

Use the **Retrieve File via TFTP** tab to upload files from the AP to the TFTP server. The TFTP server must be running and configured to point to the directory to which you want to copy the uploaded file. We suggest you assign the file a meaningful name, which may include version or location information.

If you don't have a TFTP server installed on your system, install the TFTP server from the ORiNOCO CD. You can either install the TFTP server from the CD Wizard or run **OEM-TFTP-Server.exe** found in the CD's *Xtras/SolarWinds* sub-directory.

The **Retrieve AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.

  – Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.

- **File Name:** Enter the name of the file to be uploaded.
- **File Type**: Select the type of file to be uploaded: Config file, CLI Batch File, or CLI Batch (Error) Log.

Use the following procedure to retrieve a file from an AP to a TFTP server:

1. If retrieving a Config file, configure all the required parameters in their respective tabs. Reboot the device.
2. Retrieve and store the file. Click the **Retrieve File** button to initiate the upload of the file from the AP to the TFTP server.
3. If you retrieved a Configuration file, update the file as necessary.
4. If you retrieved a CLI Batch File or CLI Batch Log, you can examine the file using a standard text editor. For more information on CLI Batch Files, see CLI Batch File.

Figure 6-7 Retrieve File via TFTP Command Screen

Retrieve File via HTTP

Use the **Retrieve File via HTTP** tab to retrieve configuration files, CLI Batch Files, or CLI Batch Logs from the AP. Select the type of file (Config, CLI Batch File, or CLI Batch Log) from the **File Type** drop-down menu.

For more information on CLI Batch Files and CLI Batch Logs see CLI Batch File.

Click on the **Retrieve File** button to initiate the operation.

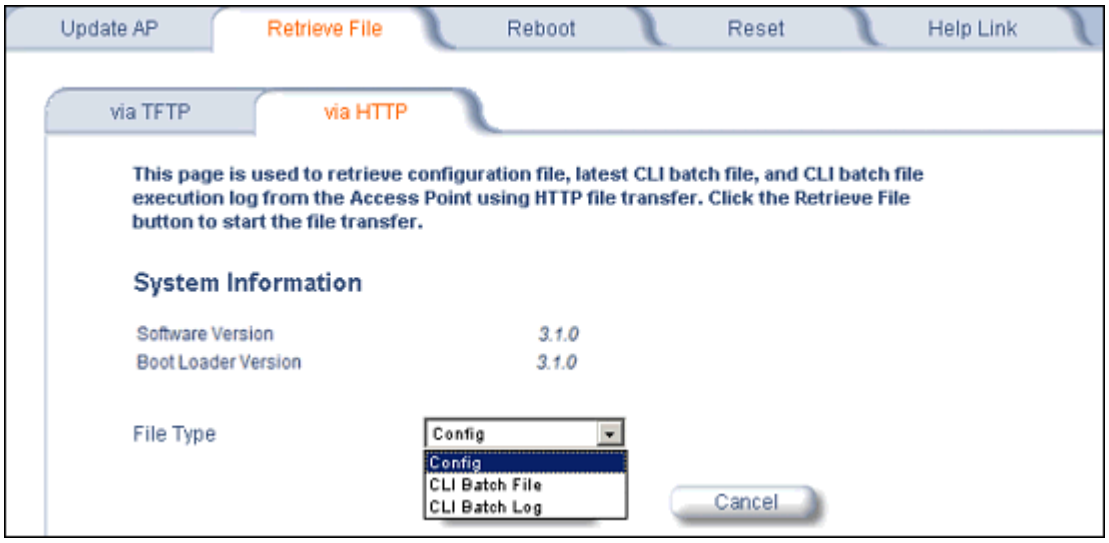


Figure 6-8 Retrieve File via HTTP Command Screen

A confirmation message is displayed, asking if the user wants to proceed with retrieving the file.

Figure 6-9 Retrieve File Confirmation Dialog

Click **OK** to continue with the operation or Cancel to abort the operation. On clicking **OK**, the File Download window appears.

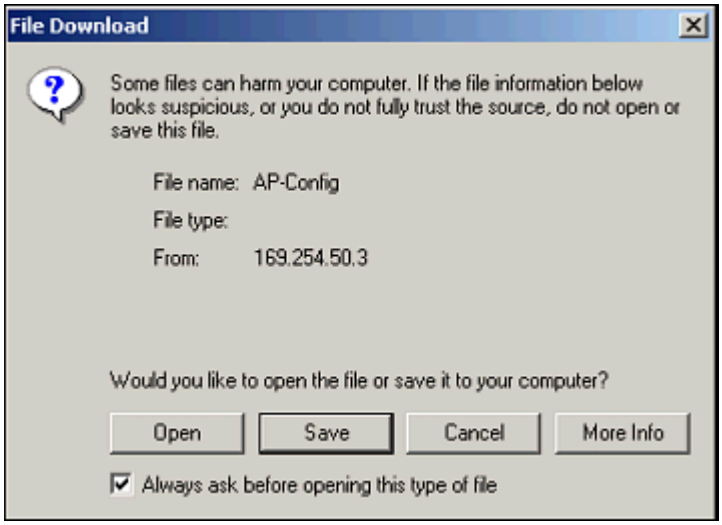


Figure 6-10 File Download Dialog Box

On clicking the **Save** button the Save As window displays, where the user is prompted to choose the filename and location where the file is to be downloaded. Select an appropriate filename and location and click **OK**.

Reboot

Use the **Reboot** tab to save configuration changes (if any) and reset the AP. Enter a value between 0 and 65535 seconds; entering a value of 0 (zero) seconds causes an immediate reboot. Note that **Reset**, described below, does not save configuration changes.

CAUTION: *Rebooting the AP will cause all users who are currently connected to lose their connection to the network until the AP has completed the restart process and resumed operation.*

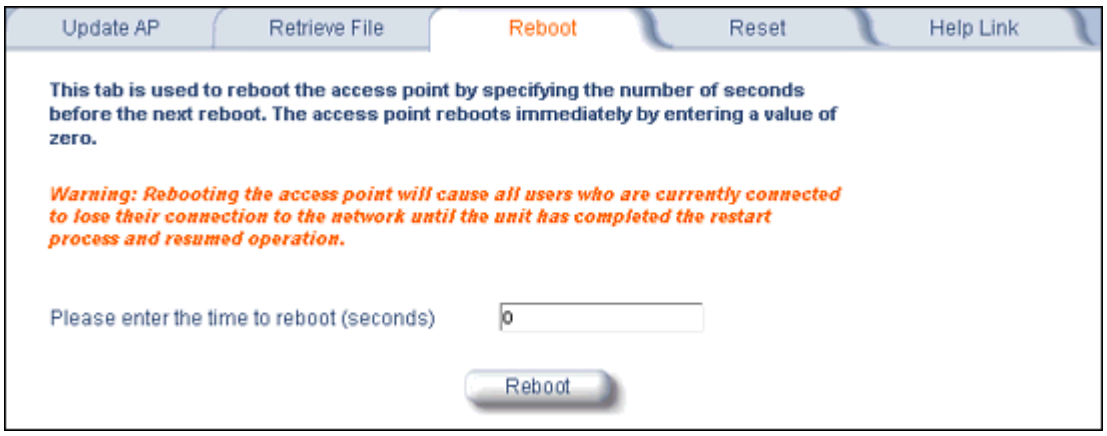


Figure 6-11 Reboot Command Screen

Reset

Use the **Reset** tab to restore the AP to factory default conditions. Since this will reset the AP's current IP address, a new IP address must be assigned. See Recovery Procedures for more information.

CAUTION: *Resetting the AP to its factory default configuration will permanently overwrite all changes that have made to the unit. The AP will reboot automatically after this command has been issued.*

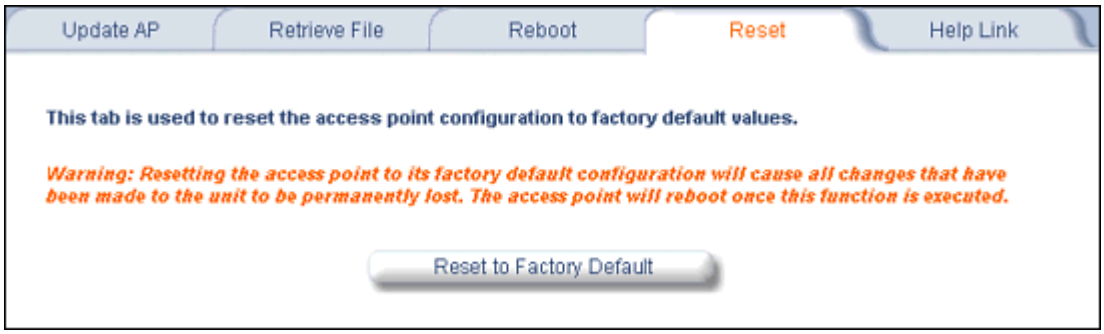


Figure 6-12 Reset to Factory Defaults Command Screen

NOTE: *The AP may also be reset from the RESET button located on the side of the unit. However, this action will not reset the unit to factory default settings.*

Help Link

Use the **Help** tab to configure the location of the AP Help files.

During initialization, the AP on-line help files are downloaded to the default location: **C:/Program Files/ORiNOCO/AP4xxxx/HTML/index.htm**.

To enable the Help button on each page of the Web interface to access the help files, however, copy the entire Help folder to a web server, then specify the new HTTP path in the **Help Link** box.

NOTE: *The configured Help Link must point to an HTTP address in order to enable the Help button on each page of the Web interface.*

NOTE: *Use the forward slash character ("/") rather than the backslash character ("\") when configuring the **Help Link** location.*

NOTE: *Add the AP's management IP address into the Internet Explorer list of Trusted Sites.*

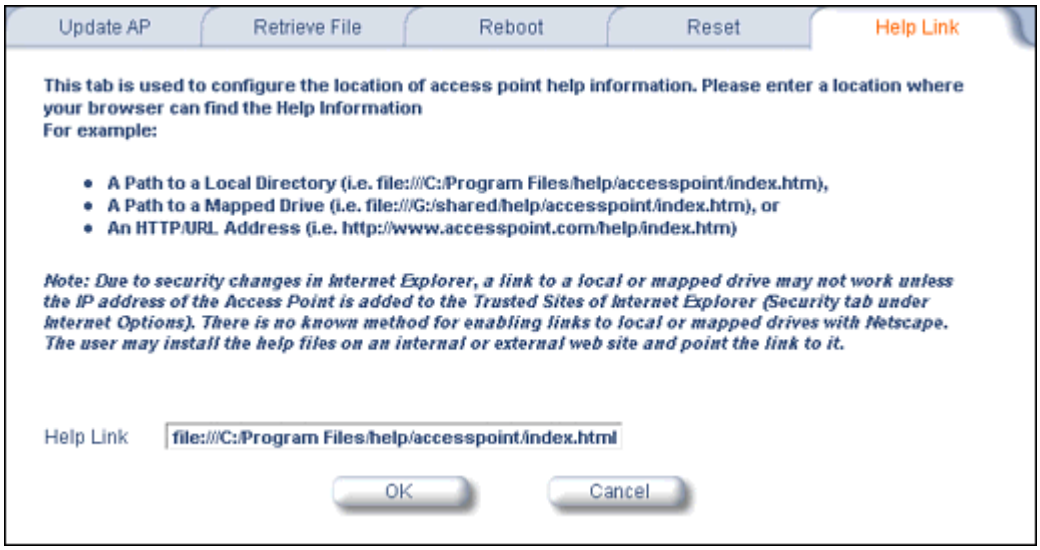


Figure 6-13 Help Link Configuration Screen

7 Troubleshooting

This chapter provides information on the following:

- Troubleshooting Concepts
- Symptoms and Solutions
- Recovery Procedures
- Related Applications

NOTE: *This section helps you locate problems related to the AP device setup. For details about RADIUS, TFTP, serial communication programs (such as HyperTerminal), Telnet applications, or web browsers, please see the documentation that came with the respective application for assistance.*

Troubleshooting Concepts

The following list identifies important troubleshooting concepts and topics. The most common initialization and installation problems relate to IP addressing. For example, you must have valid IP addresses for both the AP and the management computer to access the unit's HTTP interface.

- **IP Address management is fundamental.**
- **Factory default units are set for "Dynamic" (DHCP) IP Address assignment.** The default IP address for the AP is **169.254.128.132** if your network does not have a DHCP server. If you connect the AP to a network with an active DHCP server, then use ScanTool to locate the IP address of your unit. If a DHCP server is not active on your subnet, then use ScanTool to assign a static IP address to the unit.
- **The Trivial File Transfer Protocol (TFTP) provides a means to download and upload files.** These files include the AP Image (executable program) and configuration files.
- **If the AP password is lost or forgotten, you will need to reset to default values.** The Reset to Factory Default Procedure resets configuration, but does not change the current AP Image.
- **The AP Supports a Command Line Interface (CLI).** If you are having trouble locating your AP on the network, connect to the unit directly using the serial interface and see Command Line Interface (CLI) for CLI command syntax and parameter names.
- **ScanTool does not work over routers.** You must be connected to the same subnet/physical LAN segment to use ScanTool. Note that ScanTool also works over the wireless interface; you can run it on a wireless client connected to the target AP or an AP connected to the same LAN segment/subnet.
- **If all else fails…** Use the Forced Reload Procedure to erase the current AP Image and configuration file and then download a new image.

Symptoms and Solutions

Connectivity Issues

Connectivity issues include any problem that prevents you from powering up or connecting to the AP.

AP Unit Will Not Boot - No LED Activity

1. Make sure your power source is operating.
2. Make sure all cables are connected to the AP correctly.
3. If you are using Active Ethernet, make sure you are using a Category 5, foiled, twisted pair cable to power the AP.

Serial Link Does Not Work

1. Make sure you are using a standard, straight-through, 9-pin serial cable.
2. Double-check the physical network connections.
3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
   – Com Port: (COM1, COM2, etc. depending on your computer);
   – Baud rate: 9600; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;
   – Line Feeds with Carriage Returns
   (In HyperTerminal select:
   File > Properties > Settings > ASCII Setup > Send Line Ends with Line Feeds)

Ethernet Link Does Not Work

1. Double-check the physical network connections. Use a known-good unit to make sure the network connection is present. Once you have the AP IP address, you can use the “Ping” command over Ethernet to test the IP Address. If the AP responds to the Ping, then the Ethernet Interface is working properly.
2. By default, the Access Point will attempt to automatically detect the Ethernet settings. However, if you are having problems with the Ethernet link, manually configure the Access Point’s Ethernet settings. For example, if your switch operates at 100 Mbits/sec/Full Duplex, manually configure the Access Point to use these settings (see Ethernet). If you cannot access the unit over Ethernet, then use the CLI interface over the serial port to configure the Ethernet port (see Command Line Interface (CLI) and Set Ethernet Speed and Transmission Mode).
3. Perform network infrastructure troubleshooting (check switches, routers, etc.).

Basic Software Setup and Configuration Problems

Lost AP, Telnet, or SNMP Password

1. Perform the Reset to Factory Default Procedure in this guide. This procedure resets system and network parameters, but does not affect the AP Image.
   The default AP HTTP password is “public”. The default Telnet password and the default SNMP password are also “public”.

Client Computer Cannot Connect

1. Client computers should have the same Network Name and security settings as the AP.
2. Network Names should be allocated and maintained by the Network Administrator.
3. See the documentation that came with your client card for additional troubleshooting suggestions.

AP Has Incorrect IP Address

1. Default IP Address Assignment mode is dynamic (DHCP). If you do not have a DHCP server on your network, the default IP Address is **169.254.128.132**. If you have more than one unintialized AP connected to the network, they will all have the same default IP address and you will not be able to communicate with them (due to an IP address conflict). In this case, assign each AP a static IP address via the serial cable or turn off all units but one and change the IP address using ScanTool one at a time.
2. The AP only contacts a DHCP server during boot-up. If your network’s DHCP server is not available while the AP is booting, the device will use the default IP address (**169.254.128.132)**. Reboot the AP once your DHCP server is on-line again or use the ScanTool to find the Access Point’s current IP address.
3. To find the unit’s current IP address if using DHCP, open the IP Client Table in the DHCP Server and match the Access Point’s IP address to its MAC address (found on the product label). Alternatively, use ScanTool to identify an Access Point’s current IP address.
4. Once you have the current IP address, use the HTTP or CLI Interface to change the unit’s IP settings, if necessary.
5. If you use static IP Address assignments, and cannot access the unit over Ethernet, use the Initializing the IP Address using CLI procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration.

6. Perform the Reset to Factory Default Procedure in this guide. This will reset the unit to “DHCP” mode. If there is a DHCP Server on the network, the DHCP Server will assign an IP Address to the AP.

HTTP Interface or Telnet Interface Does Not Work

1. Make sure you are using a compatible browser:
   – Microsoft Internet Explorer 6 with Service Pack 1 or later
   – Netscape 7.1 or later
2. Make sure you have the proper IP address. Enter your Access Point’s IP Address in the browser address bar, similar to this example:
   http://192.168.1.100
   When the ***Enter Network Password*** window appears, leave the **User Name** field empty and enter the HTTP password in the **Password** field. The default HTTP password is “public”.
3. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

HTML Help Files Do Not Appear

1. Verify that the HTML Help files are installed in the default directory:
   C:\Program Files\ORiNOCO\AP4xxxx\HTML
   If the Help files are not located in this folder, contact your network administrator to find out where the Help files are located on your server.
2. Copy the entire folder to your Web server.
3. Perform the following steps to specify the path for the Help files:
   a. Click the **Commands** button in the HTTP interface.
   b. Select the **Help** tab located at the top of the screen.
   c. Enter the pathname where the Help files are located in the **Help Link** box. This must be an HTTP address.
   d. Click **OK**.

Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your AP IP address in the Telnet connection dialog, from a DOS prompt, type:
   C:\> telnet <AP IP Address>
2. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

TFTP Server Does Not Work

1. Make sure the TFTP Server has been started.
2. Verify the IP address of the TFTP Server. The server may be local or remote, so long as it has a valid IP address.
3. Configure the TFTP Server to “point” to the folder containing the file to be downloaded (or to the folder in which the file is to be uploaded).
4. Verify that you have entered the proper AP Image file name (including the file extension) and directory path (if needed).
5. If you have a problem uploading a file, verify that the TFTP server is configured to allow uploads (typically the default setting is to allow only downloads).

Client Connection Problems

Client Software Finds No Connection

Make sure you have configured your client software with the proper Network Name and Security settings. Network Names and WEP Keys are typically allocated and maintained by your network administrator.

Client PC Card Does Not Work

1. Make sure you are using the latest PC Card driver software.
2. Download and install the latest *ORiNOCO* client software from http://support.proxim.com.

Intermittent Loss of Connection

1. Make sure you are within range of an active AP.
2. You can check the signal strength using the signal strength gauge on your client software.

Client Does Not Receive an IP Address - Cannot Connect to Internet

1. If the AP is configured as a DHCP server, open the Web-browser Interface and select the **Configure** button and then the **Network** tab to make sure the proper DHCP settings are being used.
2. If you are not using the DHCP server feature on the AP, then make sure that your local DHCP server is accessible from the Access Point's subnet.
3. If using Active Ethernet, make sure you are not using a crossover Ethernet cable between the AP and the hub.

VLAN Operation Issues

Verifying Proper Operation of the VLAN Feature

The correct VLAN configuration can be verified by "pinging" both wired and wireless hosts from both sides of the AP device and the network switch. Traffic can be "sniffed" on both the wired (Ethernet) and wireless (WDS) backbones (if configured). Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the AP.

NOTE: *The AP-4000/4000M/4900M supports 16 VLAN/SSID pairs per wireless interface, each with a configured security profile.*

VLAN Workgroups

The correct VLAN assignment can be verified by pinging the AP to ensure connectivity, by pinging the switch to ensure VLAN properties, and by pinging hosts past the switch to confirm the switch is functional. Ultimately, traffic can be "sniffed" on the Ethernet or WDS interfaces (if configured) using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the user's assigned network name.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a Forced Reload is necessary. See Forced Reload Procedure.
- Workaround: you can configure the switch to mimic the nonexistent host.

I have just configured the Management ID and now I can't manage the AP?

- Check to ensure your password is correct. If your password is incorrect or all inbound packets do NOT have the correct tag, then a Forced Reload is necessary. See Forced Reload Procedure.

CAUTION: *The* Forced Reload Procedure *disconnects all users and resets all values to factory defaults.*

Active Ethernet (AE)

The AP Does Not Work

1. Verify that you are using a standard UTP Category 5 cable.
2. Try a different port on the same AE hub (remember to move the input port accordingly) – if it works, there is probably a faulty port or bad RJ-45 port connection.

3. If possible, try to connect the AP to a different AE hub.
4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ-45 connection.
5. Check power plug and hub.
6. If the Ethernet link goes down, check the cable, cable type, switch, and hub.

There Is No Data Link

1. Verify that the indicator for the port is “on.”
2. Verify that the AE hub is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5 or better and is less than 100 meters (approximately 325 feet) in length from the Ethernet source to the AP.
4. Try to connect a different device to the same port on the AE hub – if it works and a link is established, there is probably a faulty data link in the AP.
5. Try to re-connect the AP to a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the AE hub or a bad RJ-45 connection.

“Overload” Indications

1. Verify that you are not using a cross-over cable between the AE output port and the AP.
2. Verify that there is no short over any of the twisted pair cables.
3. Move the device into a different output port (remember to move the input port accordingly); if it works, there is probably a faulty port or bad RJ-45 connection.

Recovery Procedures

The most common installation problems relate to IP addressing. For example, without the TFTP server IP Address, you will not be able to download a new AP Image to the AP. IP Address management is fundamental. We suggest you create a chart to document and validate the IP addresses for your system.

If the password is lost or forgotten, you will need to reset the AP to default values. The Reset to Factory Default Procedure resets configuration settings, but does not change the current AP Image.

If the AP has a corrupted software image, follow the Forced Reload Procedure to erase the current AP Image and download a new image.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration values, including the Access Point’s IP address and subnet mask. The current AP Image is not deleted. Follow this procedure if you forget the Access Point’s password:

1. Press and hold the **RELOAD** button for 10 seconds.

NOTE: *You need to use a pin or the end of a paperclip to press a button.*

   The AP reboots, and the factory default network values are restored.
2. If not using DHCP, use the ScanTool or use CLI over a serial connection to set the IP address, subnet mask, and other IP parameters. See Command Line Interface (CLI) for CLI information.

Forced Reload Procedure

Use this procedure to erase the current AP Image and configuration file and download a new AP Image. In some cases, specifically when a missing or corrupted AP Image prevents successful booting, you may need to use ScanTool or the Bootloader CLI to download a new executable AP Image.

For this procedure, you will first erase the AP Image currently installed on the unit and then use either ScanTool or the Bootloader CLI (over the serial port) to set the IP address and download a new AP Image. Follow these steps:

1. While the unit is running, press the **RESET** button.

   NOTE: *You need to use a pin or the end of a paperclip to press a button.*

   The AP reboots and the indicators begin to flash.

CAUTION: *By completing Step 2, the firmware in the AP will be erased. You will need an Ethernet connection, a TFTP server, and a serial cable (if using the Bootloader CLI) to reload firmware.*

2. Press and hold the **RELOAD** button for about 20 seconds until the **POWER LED** turns amber.

   The AP deletes the current AP Image.

3. Follow one of the procedures below to load a new AP Image to the Access Point:
   - Download a New Image Using ScanTool
   - Download a New Image Using the Bootloader CLI

Download a New Image Using ScanTool

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides and to a computer that is running ScanTool (this is either two separate computers connected to the same network or a single computer running both programs).

ScanTool detects if an Access Point does not have a valid software image installed. In this case, the **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's ***Change*** screen so you can download a new image to the unit. (These fields are grayed out if ScanTool does not detect a software image problem.)

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

Follow these steps to use ScanTool to download a software image to an Access Point with a missing image:

1. Download the latest software from http://support.proxim.com (Knowledgebase Answer ID **1250)**.
1. Copy the latest software updates to your TFTP server.
2. Launch ScanTool.
3. Highlight the entry for the AP you want to update and click **Change**.
4. Set **IP Address Type** to **Static**.

NOTE: *You need to assign static IP information temporarily to the Access Point since its DHCP client functionality is not available when no image is installed on the device.*

5. Enter an unused IP address that is valid on your network in the **IP Address** field. You may need to contact your network administrator to get this address.
6. Enter the network's **Subnet Mask** in the field provided.
7. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your network administrator to get this address. You should only need to enter the default gateway address (169.254.128.133) if the Access Point and the TFTP server are separated by a router.
8. Enter the IP address of your TFTP server in the field provided.
9. Enter the **Image File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
10. Click **OK**.

The Access Point will reboot and the download will begin automatically. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

11. Click **OK** when prompted that the device has been updated successfully to return to the ***Scan List*** screen.
12. Click **Cancel** to close the ScanTool.
13. When the download process is complete, configure the AP as described in Installation and Initialization and Advanced Configuration.

Download a New Image Using the Bootloader CLI

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the AP with a cross-over Ethernet cable.

You must also connect the AP to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP address and download an AP Image.

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

1. Download the latest software from http://support.proxim.com (Knowledgebase Answer ID **1250)**.
2. Copy the latest software updates to your TFTP server's default directory.
3. Use a straight-through serial cable to connect the Access Point's serial port to your computer's serial port.
4. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
5. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.

   HyperTerminal sends a line return at the end of each line of code.
6. Press the **RESET** button on the AP.

   The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Sending Traps to SNMP manager periodically.** After this message appears, press the **ENTER** key repeatedly until the following prompt appears:

   `[Device name]>`
7. Enter only the following statements:

   `[Device name]>` **`show`** (to view configuration parameters and values)

   `[Device name]>` **`set ipaddrtype static`**

   `[Device name]>` **`set ipaddr <Access Point IP Address>`**

   `[Device name]>` **`set ipsubmask <IP Mask>`**

   `[Device name]>` **`set tftpipaddr <TFTP Server IP Address>`**

   `[Device name]>` **`set tftpfilename <AP Image File Name, including file extension>`**

   `[Device name]>` **`set ipgw <Gateway IP Address>`**

   `[Device name]>` **`show`** (to confirm your new settings)

```
[Device name]> reboot
```

Example:

```
[Device name]> show
[Device name]> set ipaddrtype static
[Device name]> set ipaddr 10.0.0.12
[Device name]> set ipsubmask 255.255.255.0
[Device name]> set tftpipaddr 10.0.0.20
[Device name]> set tftpfilename MyImage.bin
[Device name]> set ipgw 10.0.0.30
[Device name]> show
[Device name]> reboot
```

The AP will reboot and then download the image file. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

8. When the download process is complete, configure the AP as described in Installation and Initialization and Advanced Configuration.

Setting IP Address using Serial Port

Use the following procedure to set an IP address over the serial port using the CLI. The network administrator typically provides the AP IP address.

Hardware and Software Requirements

- Standard straight-through serial data (RS-232) cable with a one male DB-9 connector and one female DB-9 connector. The AP comes with a female 9-pin serial port.
- ASCII Terminal software, such as HyperTerminal.

Attaching the Serial Port Cable

1. Connect one end of the serial cable to the AP and the other end to a serial port on your computer.
2. Power on the computer and AP, if necessary.

Initializing the IP Address using CLI

After installing the serial port cable, you may use the CLI to communicate with the AP. CLI supports most generic terminal emulation programs, such as HyperTerminal (which is included with the Windows operating systems). In addition, many web sites offer shareware or commercial terminal programs you can download. Once the IP address has been assigned, you can use the HTTP interface or the CLI over Telnet to complete configuration.

Follow these steps to assign the AP an IP address:

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.

   HyperTerminal sends a line return at the end of each line of code.
3. Press the **RESET** button on the AP.

The terminal display shows Power On Self Tests (POST) activity, and then displays a CLI prompt, similar to the example below. This process may take up to 90 seconds.

```
[Device name]> Please enter password:
```

4. Enter the CLI password (default is **public**).

   The terminal displays a welcome message and then the CLI Prompt:

   ```
   [Device name]>
   ```

5. Enter **show ip**. Network parameters appear:

```
[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Figure 7-1 Result of "show ip" CLI Command

6. Change the IP address and other network values using **set** and **reboot** CLI commands, similar to the example below (use your own IP address and subnet mask). Note that IP Address Type is set to Dynamic by default. If you have a DHCP server on your network, you should not need to manually configure the Access Point's IP address; the Access Point will obtain an IP address from the network's DHCP server during boot-up.

   After each entry the CLI reminds you to reboot; however wait to reboot until all commands have been entered.

   ```
   [Device name]> set ipaddrtype static
   [Device name]> set ipaddr <IP Address>
   [Device name]> set ipsubmask <IP Subnet Mask>
   [Device name]> set ipgw <Default Gateway IP Address>
   [Device name]> show ip (to confirm your new settings)
   [Device name]> reboot 0
   ```

7. After the AP reboots, verify the new IP address by reconnecting to the CLI and enter a **show ip** command. Alternatively, you can ping the AP from a network computer to confirm that the new IP address has taken effect.
8. When the proper IP address is set, use the HTTP interface or CLI over Telnet to configure the rest of the unit's operating parameters.

Related Applications

RADIUS Authentication Server

If you enabled RADIUS Authentication on the AP, make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log in. There are several reasons the authentication server services might be unavailable, here are two typical things to check:

- Make sure you have the proper RADIUS authentication server information setup configured in the AP. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813).
- Make sure the RADIUS authentication server RAS setup matches the AP.

TFTP Server

The “Trivial File Transfer Protocol” (TFTP) server allows you to transfer files across a network. You can upload configuration files from the AP for backup or copying, and you can download configuration files or new software images. The TFTP software is located on the ORiNOCO AP Installation CD-ROM.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP address. Note that you do not need a TFTP server running unless you want to transfer files to or from the AP.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP Address, the proper AP Image file name, and that the TFTP server is connected.
- Make sure the TFTP server is configured to both send and receive, with no time-out.

Command Line Interface (CLI)

A

This section discusses the following:

- General Notes
- Command Line Interface (CLI) Variations
- CLI Command Types
- Using Tables and Strings
- Configuring the AP using CLI commands
- Set Basic Configuration Parameters using CLI Commands
- Other Network Settings
- CLI Monitoring Parameters
- Parameter Tables
- CLI Batch File

CLI commands can be used to initialize, configure, and manage the Access Point.

- CLI commands may be entered in real time through a keyboard or submitted with CLI scripts.
- A *CLI Batch file* is a user-editable configuration file that provides a user-friendly way to change the AP configuration through a file upload. The CLI Batch file is an ASCII file that facilitates Auto Configuration because it does not require the user to access one of the AP's management interfaces to make configuration changes as is required with the proprietary LTV format configuration file.
- The CLI is available through both the Serial Port interface and over the Ethernet interface using Telnet.

NOTE: *All CLI commands and parameters are case-sensitive.*

General Notes

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts, network access infrastructures, and client-server relationships. In addition, you should be familiar with software setup procedures for typical network operating systems and servers.

Notation Conventions

- Computer prompts are shown as constant width type. For example: `[Device-Name]>`
- Information that you input as shown is displayed in bold constant width type. For example: `[Device name]> set ipaddr 10.0.0.12`
- The names of keyboard keys, software buttons, and field names are displayed in bold type. For example: Click the **Configure** button.
- Screen names are displayed in bold italics. For example, the ***System Status*** screen.

Important Terminology

- Configuration Files - Database files containing the current Access Point configuration. Configuration items include the IP Address and other network-specific values. Config files may be downloaded to the Access Point or uploaded for backup or troubleshooting.

- Download vs. Upload - Downloads transfer files to the Access Point. Uploads transfer files from the Access Point. The TFTP server performs file transfers in both directions.
- Group - A logical collection of network parameter information. For example, the System Group is composed of several related parameters. Groups can also contain Tables. All items for a given Group can be displayed with a **show <Group>** CLI Command.
- Image File - The Access Point software executed from RAM. To update an Access Point you typically download a new Image File. This file is often referred to as the “AP Image”.
- Parameter - A fundamental network value that can be displayed and may be changeable. For example, the Access Point must have a unique IP Address and the Wireless interface must be assigned an SSID. Change parameters with the CLI **set** Command, and view them with the CLI **show** Command.
- Table - Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP Table. All items for a given Table can be displayed with a **show <Table>** CLI Command.
- TFTP - Refers to the TFTP Server, used for file transfers.

Navigation and Special Keys

This CLI supports the following navigation and special key functions to move the cursor along the prompt line.

Key Combination	Operation
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on
Ctrl-U	Delete all text to left of cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Tab	Complete the command line
?	List available commands

CLI Error Messages

The following table describes the error messages associated with improper inputs or expected CLI behavior.

Error Message	Description
Syntax Error	Invalid syntax entered at the command prompt.
Invalid Command	A non-existent command has been entered at the command prompt.
Invalid Parameter Name	An invalid parameter name has been entered at the command prompt.
Invalid Parameter Value	An invalid parameter value has been entered at the command prompt.
Invalid Table Index	An invalid table index has been entered at the command prompt.
Invalid Table Parameter	An invalid table parameter has been entered at the command prompt.
Invalid Table Parameter Value	An invalid table parameter value has been entered at the command prompt.
Read Only Parameter	User is attempting to configure a read-only parameter.
Incorrect Password	An incorrect password has been entered in the CLI login prompt.
Download Unsuccessful	The download operation has failed due to incorrect TFTP server IP Address or file name.
Upload Unsuccessful	The upload operation has failed due to incorrect TFTP server IP Address or file name.

Command Line Interface (CLI) Variations

Administrators use the CLI to control Access Point operation and monitor network statistics. The AP supports two types of CLI: the Bootloader CLI and the normal CLI. The Bootloader CLI provides a limited command set, and is used when the current AP Image is bad or missing. The Bootloader CLI allows you to assign an IP Address and download a new image. Once the image is downloaded and running, the Access Point uses the normal CLI. This guide covers the normal CLI unless otherwise specified.

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the AP. This interface is only accessible via the serial interface if the AP does not contain a software image or a download image command over TFTP has failed.

The Bootloader CLI provides you with the ability to configure the initial setup parameters as well as download a software image to the device.

The following functions are supported by the Bootloader CLI:

- configuration of initial device parameters using the **set** command
- **show** command to view the device's configuration parameters
- **help** command to provide additional information on all commands supported by the Bootloader CLI
- **reboot** command to reboot the device

The parameters supported by the Bootloader CLI (for viewing and modifying) are:

- System Name
- IP Address Assignment Type
- IP Address
- IP Mask
- Gateway IP Address
- TFTP Server IP Address
- Image File Name (including the file extension)

The following lists display the results of using the **help** command in the Bootloader CLI:

```
[Device name]> help

Command List        Description
============        ===========
set                 Set system parameters
show                Show running system information
help                Description of commands, command usage and parameters
reboot              reboot the target

Command Usage
=============
set <parameter name> <parameter value> <cr>
show <cr>
help <cr>
reboot <cr>

Parameter List      Description
==============      ===========
sysname             System Name
ipaddr              System IP Address
ipsubmask           System Subnet Mask
ipgw                System Default Gateway IP Address
tftpipaddr          TFTP Server IP Address
tftpfilename        Image or Binary File name
ipaddrtype          System IP Address Type - STATIC or DYNAMIC

[Device name]>
```

Figure A-1 Results of "help" bootloader CLI command

The following lists display the results of using the **show** command in the Bootloader CLI:

```
[Device name]> show

sysname          Device name          System Name
ipaddr           10.0.0.1             System IP Address
ipsubmask        255.0.0.0            System Subnet Mask
ipgw             10.0.0.1             System Default Gateway IP Address
ipaddrtype       DYNAMIC              IP Address type
tftpipaddr       10.0.0.2             TFTP Server IP Address
tftpfilename     FILENAME             Image or Binary File Name

[Device name]>
```

Figure A-2 Results of "show" bootloader CLI command

CLI Command Types

This guide divides CLI Commands into two categories: Operational and Parameter Controls.

Operational CLI Commands

These commands affect Access Point behavior, such as downloading, rebooting, and so on. After entering commands (and parameters, if any) press the **Enter** key to execute the Command Line.

Operational commands include:

- **?:** Typing a question mark lists CLI Commands or parameters, depending on usage (you do not need to type Enter after typing this command)
- **done, exit, quit:** Terminates the CLI session
- **download:** Uses a TFTP server to download "image" files, "config" files, "bootloader upgrade" files, a "license" file, "SSL certificates", "SSL private keys", "SSH public keys", "SSH private keys", or "CLI Batch Files" to the Access Point
- **help:** Displays general CLI help information or command help information, such as command usage and syntax
- **history:** Remembers commands to help avoid re-entering complex statements
- **passwd:** Sets the Access Point's CLI password
- **reboot:** Reboots the Access Point in the specified time
- **search:** Lists the parameters in a specified Table
- **upload:** Uses TFTP server to upload "config" files from Access Point to TFTP default directory or specified path

? (List Commands)

This command can be used in a number of ways to display available commands and parameters.

The following table lists each operation and provides a basic example. Following the table are detailed examples and display results for each operation.

Operation	Basic Example
Display the Command List (Example 1)	`[Device-Name]>?`
Display commands that start with specified letters (Example 2)	`[Device-Name]>s?`
Display parameters for set and show Commands (Examples 3a and 3b)	`[Device-Name]>set ?` `[Device-Name]>show ipa?`
Prompt to enter successive parameters for Commands (Example 4)	`[Device-Name]>download ?`

Example 1. Display Command list

To display the Command List, enter **?**.

[Device-Name]>**?**

```
[Device Name]>
show
set
download
upload
reboot
passwd
help
quit
done
exit
history
search
[Device Name]> _
```

Figure A-3 Result of "?" CLI command

Example 2. Display specific Commands

To show all commands that start with specified letters, enter one or more letters, then **?** with no space between letters and **?**.

[Device-Name]>**s?**

```
[Device Name]> s
show                set                 search
```

Figure A-4 Result of "s?" CLI command

Example 3. Display parameters for set and show

Example 3a allows you to see every possible parameter for the set (or show) commands. Notice from example 3a that the list is very long. Example 3b shows how to display a subset of the parameters based on initial parameter letters.

Example 3a. Display every parameter that can be changed

[Device-Name]>**set ?**

```
[Device Name]> set
Command Description:
The set command modifies the value of a given scalar parameter or table entry.

Command Usage:
set <parameter> <parameter value> <CR>
set <table> <index> <arg1> <value1> ..... <argN> <valueN> <CR>

Example:
set sysname "My Wireless Device" <CR>
set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0 cmt "Test WorkStation"
 <CR>

[Device Name]> set
broadcastfltbl
dhcpgw
dhcpippooltbl
dhcppridnsipaddr
dhcpsecdnsipaddr
dhcpstatus
dnsdomainname
dnsprisvripaddr
dnssecsvripaddr
dnsstatus
etherfltifbitmask
.
.
.
.
telsessiontout
tftpfilename
tftpfiletype
tftpipaddr
vlanidtbl
vlanmgmtid
vlanstatus
wdstbl
wif
wifsec
[Device Name]> set _
```

Figure A-5 Result of "set ?" CLI command

Example 3b. Display parameters based on letter sequence

This example shows entries for parameters that start with the letter "i". The more letters you enter, the fewer the results returned. Notice that there is no space between the letters and the question mark.

```
[Device-Name]> show ipa?
```

```
[Device Name]> show ipa
ipaddr              ipaddrtype          iparp
iparpfltipaddr      iparpfltstatus      iparpfltsubmask
```

Figure A-6 Result of "show ipa?" CLI command

```
[Device-Name]> show iparp?
```

```
[Device Name]> show iparp
iparp               iparpfltipaddr      iparpfltstatus
iparpfltsubmask
[Device Name]> show iparp_
```

Figure A-7 Result of "show iparp?" CLI command

Example 4. Display Prompts for Successive Parameters

Enter the command, a space, and then **?**. Then, when the parameter prompt appears, enter the parameter value. The parameter is changed and a new CLI line is echoed with the new value (in the first part of the following example, the value is the IP Address of the TFTP server).

After entering one parameter, you may add another **?** to the new CLI line to see the next parameter prompt, and so on until you have entered all of the required parameters. The following example shows how this is used for the **download** Command. The last part of the example shows the completed **download** Command ready for execution.

```
[Device-Name]> download ?
<TFTP IP Address>

[Device-Name]> download 192.168.0.101 ?
<File Name>

[Device-Name]> download 192.168.0.101 apimage ?
<file type (config/img/bootloader)>

[Device-Name]> download 192.168.0.101 apimage img <CR>
```

done, exit, quit

Each of the following commands ends a CLI session:

```
[Device-Name]> done
[Device-Name]> exit
[Device-Name]> quit
```

download

Downloads the specified file from a TFTP server to the Access Point. Executing **download** in combination with the asterisks character ("*") will make use of the previously set TFTP parameters. Executing download without parameters will display command help and usage information.

1. Syntax to download a file:
   `[Device-Name]>download <tftp server address> <path and filename> <file type>`

Example:
[Device-Name]>**download 192.168.1.100 APImage2 img**

2. Syntax to display help and usage information:
[Device-Name]>**download**

3. Syntax to execute the download Command using previously set (stored) TFTP Parameters:
[Device-Name]>**download ***

help

Displays instructions on using control-key sequences for navigating a Command Line and displays command information and examples.

1. Using help as the only argument:
[Device-Name]>**help**

```
[Device Name]> help
Type ? at the command prompt for a command list.

Complete command description and command usage can be provided by:
help <command name> <CR>
<command name> help <CR>

Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W ..... delete previous word
Ctrl-T ..... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer

Tab     .... will attempt command completion
# .... Comment Character
?       .... will provide command listing

Examples:
 '?'            list all the supported commands
'sh?'           list all commands that start with sh
'show ?'        list all arguments to the show command
'sh<TAB>'       complete the 'show' command

[Device Name]>
```

Figure A-8 Results of "help" CLI command

2. Complete command description and command usage can be provided by:
[Device-Name]>**help <command name>**
[Device-Name]>**<command name> help**

history

Shows content of Command History Buffer. The Command History Buffer stores command statements entered in the current session. To avoid re-entering long command statements, use the keyboard "up arrow" (Ctrl-P) and "down arrow" (Ctrl-N) keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the **Enter** key to execute, or you may edit the statement before executing it.

[Device-Name]> **history**

passwd

Changes the CLI Password.

[Device-Name]> **passwd oldpassword newpassword newpassword**

reboot

Reboots Access Point after specified number of seconds. Specify a value of 0 (zero) for immediate reboot.

```
[Device-Name]> reboot 0
[Device-Name]> reboot 30
```

search

Lists the parameters supported by the specified table. This list corresponds to the table information displayed in the HTTP interface. In this example, the CLI returns the list of parameters that make up an entry in the IP Access Table.

```
[Device-Name]> search mgmtipaccesstbl
```

```
[Device Name]> search mgmtipaccesstbl
The supported elements are:
index
ipaddr
ipmask
cmt
status
```

Figure A-9 Results of "search mgmtipaccesstbl" CLI command

upload

Uploads a text-based configuration file from the AP to the TFTP Server. Executing **upload** with the asterisk character ("*") will make use of the previously set/stored TFTP parameters. Executing **upload** without parameters will display command help and usage information.

1. Syntax to upload a file:
   ```
   [Device-Name]>upload <tftp server address> <path and filename> <filetype>
   ```
   Example:
   ```
   [Device-Name]>upload 192.168.1.100 APconfig.sys config
   ```

2. Syntax to display help and usage information:
   ```
   [Device-Name]>help upload
   ```

3. Syntax to execute the upload command using previously set (stored) TFTP Parameters:
   ```
   [Device-Name]>upload *
   ```

Parameter Control Commands

The following sections cover the two Parameter Control Commands (**show** and **set**) and include several tables showing parameter properties. These commands allow you to view (**show**) all parameters and statistics and to change (**set**) parameters.

- **show:** To see any Parameter or Statistic value, you can specify a single parameter, a Group, or a Table.
- **set:** Use this CLI Command to change parameter values. You can use a single CLI statement to modify Tables, or you can modify each parameter separately.

"show" CLI Command

Displays the value of the specified parameter, or displays all parameter values of a specified group (parameter table). Groups contain Parameters and Tables. Tables contain parameters for a series of similar entities.

To see a definition and syntax example, type only **show** and then press the **Enter** key. To see a list of available parameters, enter a question mark (**?**) after **show** (example: **show ?**).

Syntax:
[Device-Name]>**show <parameter>**
[Device-Name]>**show <group>**
[Device-Name]>**show <table>**

Examples:
[Device-Name]>**show ipaddr**
[Device-Name]>**show network**
[Device-Name]>**show mgmtipaccesstbl**

"set" CLI Command

Sets (modifies) the value of the specified parameter. To see a definition and syntax example, type only **set** and then press the **Enter** key. To see a list of available parameters, enter a space, then a question mark (**?**) after **set** (example: **set?**).

Syntax:
[Device-Name]>**set <parameter> <value>**
[Device-Name]>**set <table> <index> <argument 1> <value 1> ... <argument N> <value N>**

Example:

[Device-Name]>**set sysloc "Main Lobby"**
[Device-Name]>**set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0**

Configuring Objects that Require Reboot

Certain objects supported by the Access Point require a device reboot in order for the changes to take effect. In order to inform the end-user of this behavior, the CLI provides informational messages when the user has configured an object that requires a reboot. The following messages are displayed as a result of the configuring such object or objects.

Example 1: Configuring objects that require the device to be rebooted

The following message is displayed every time the user has configured an object that requires the device to be rebooted.

[Device-Name]>**set ipaddr 135.114.73.10**
The following elements require reboot

ipaddr

Example 2: Executing the "exit", "quit", or "done" commands when an object that requires reboot has been configured

In addition to the above informational message, the CLI also provides a message as a result of the **exit**, **quit**, or **done** command if changes have been made to objects that require reboot. If you make changes to objects that require reboot and execute the exit command the following message is displayed:

[Device-Name]>**exit**<CR> OR **quit**<CR> OR **done**<CR>

Modifications have been made to parameters that require the device to be rebooted. These changes will only take effect after the next reboot.

"set" and "show" Command Examples

In general, you will use the CLI **show** Command to view current parameter values and use the CLI **set** Command to change parameter values. As shown in the following examples, parameters may be set individually or all parameters for a given table can be set with a single statement.

Example 1 - Set the Access Point IP Address Parameter

Syntax:
[Device-Name]>**set <parameter name> <parameter value>**

Example:
[Device-Name]> **set ipaddr 10.0.0.12**

IP Address will be changed when you reboot the Access Point. The CLI reminds you when rebooting is required for a change to take effect. To reboot immediately, enter **reboot 0** (zero) at the CLI prompt.

Example 2 - Create a table entry or row

Use 0 (zero) as the index to a table when creating an entry. When creating a table row, only the mandatory table elements are required (comment is usually an optional table element). For optional table elements, the default value is generally applied if you do not specify a value.

Syntax:
[Device-Name]>**set <table name> <table index> <element 1> <value 1>** …
<element n> <value n>

Example:
[Device-Name]> **set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0**

A new table entry is created for IP address 10.0.0.10 with a 255.255.0.0 subnet mask.

Example 3 - Modify a table entry or row

Use the index to be modified and the table elements you would like to modify. For example, suppose the IP Access Table has one entry and you wanted to modify the IP address:

[Device-Name]>**set mgmtipaccesstbl 1 ipaddr 10.0.0.11**

You can also modify several elements in the table entry. Enter the index number and specific table elements you would like to modify. (Hint: Use the search Command to see the elements that belong to the table.)

[Device-Name]>**set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask 255.255.255.248**
cmt "First Row"

Example 4 - Enable, Disable, or Delete a table entry or row

The following example illustrates how to manage the second entry in a table.

Syntax:
[Device-Name]>**set <Table> index status <enable, disable, delete>**
[Device-Name]>**set <Table> index status <1=enable, 2=disable, 3=delete>**

Example:
[Device-Name]>**set mgmtipaccesstbl 2 status enable**
[Device-Name]>**set mgmtipaccesstbl 2 status disable**
[Device-Name]>**set mgmtipaccesstbl 2 status delete**
[Device-Name]>**set mgmtipaccesstbl 2 status 2**

NOTE: *You may need to enable a disabled table entry before you can change the entry's elements.*

Example 5 - Show the Group Parameters

This example illustrates how to view all elements of a group or table.

Syntax:
`[Device-Name]>` **`show <group name>`**

Example:
`[Device-Name]>`**`show network`**

The CLI displays network group parameters. Note **`show network`** and **`show ip`** return the same data.

```
[Device Name]> show network
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Figure A-10 Results of “show network” and “show ip” CLI Commands

Example 6 - Show Individual and Table Parameters

1. View a single parameter.

Syntax:
`[Device-Name]>`**`show <parameter name>`**

Example:
`[Device-Name]>` **`show ipaddr`**

Displays the Access Point IP address.

```
[Device Name]> show ipaddr
ipaddr

10.0.0.1

[Device Name]> _
```

Figure A-11 Result of “show ipaddr” CLI Command

2. View all parameters in a table.

Syntax:
`[Device-Name]>` **`show <table name>`**
Example: `[Device-Name]>` **`show mgmtipaccesstbl`**

The CLI displays the IP Access Table and its entries.

Using Tables and Strings

Working with Tables

Each table element (or parameter) must be specified, as in the example below.

```
[Device-Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Below are the rules for creating, modifying, enabling/disabling, and deleting table entries.

- Creation
  - The table name is required.
  - The table index is required – for table entry/instance creation the index is always zero (0).
  - The order in which the table arguments or objects are entered in not important.
  - Parameters that are not required can be omitted, in which case they will be assigned the default value.
- Modification
  - The table name is required.
  - The table index is required – to modify the table, “index” must be the index of the entry to be modified.
  - Only the table objects that are to be modified need to be specified. Not all the table objects are required.
  - If multiple table objects are to be modified the order in which they are entered is not important.
  - If the entire table entry is to be modified, all the table objects have to be specified.
- Enabling/Disabling
  - The table name is required.
  - The table index is required – for table enabling/disabling the index should be the index of the entry to be enabled/disabled.
  - The entry’s new state (either “enable” or “disable”) is required.
- Deletion
  - The table name is required.
  - The table index is required – for table deletion the index should be the index of the entry to be deleted.
  - The word “delete” is required.

Using Strings

Since there are several string objects supported by the AP, a string delimiter is required for the strings to be interpreted correctly by the command line parser. For this CLI implementation, the single quote or double quote character can be used at the beginning and at the end of the string.

For example:
`[Device-Name]>` **`set sysname Lobby`** - Does not need quote marks
`[Device-Name]>` **`set sysname "Front Lobby"`** - Requires quote marks.

The scenarios supported by this CLI are:

“My Desk in the office”	Double Quotes
‘My Desk in the office’	Single Quotes
“My ‘Desk’ in the office”	Single Quotes within Double Quotes
‘My “Desk” in the office’	Double Quotes within Single Quotes
“Daniel’s Desk in the office”	One Single Quote within Double Quotes
‘Daniel”s Desk in the office’	One Double Quote within Single Quotes

The string delimiter does not have to be used for every string object. The single quote or double quote only has to be used for string objects that contain blank space characters. If the string object being used does not contain blank spaces, then the string delimiters, single or double quotes, mentioned in this section are not required.

Configuring the AP using CLI commands

Log into the AP using HyperTerminal

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.
   HyperTerminal sends a line return at the end of each line of code.
3. Enter the CLI password (default is **public**).

NOTE: *Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, see* Change Passwords*.*

Log into the AP using Telnet

The CLI commands can be used to access, configure, and manage the AP using Telnet. Follow these steps:

1. Confirm that your computer's IP address is in the same IP subnet as the AP.

NOTE: *If you have not previously configured the Access Point's IP address and do not have a DHCP server on the network, the Access Point will default to an IP address of 169.254.128.132.*

2. Go to the DOS command prompt on your computer.
3. Type **telnet <IP Address of the unit>**.
4. Enter the CLI password (default is **public**).

NOTE: *Proxim recommends changing your default passwords immediately. To perform this operation using CLI commands, see* Change Passwords*.*

Set Basic Configuration Parameters using CLI Commands

There are a few basic configuration parameters that you may want to setup right away when you receive the AP. For example:

- Set System Name, Location and Contact Information
- Set Static IP Address for the AP
- Download an AP Configuration File from your TFTP Server
- Set up Auto Configuration
- Set Network Names for the Wireless Interface
- Enable 802.11d Support and Set the Country Code
- Enable and Configure TX Power Control for the Wireless Interface(s)
- Configure SSIDs (Network Names), VLANs, and Profiles

- Download an AP Configuration File from your TFTP Server
- Backup your AP Configuration File

Set System Name, Location and Contact Information

```
[Device-Name]>set sysname <system name> sysloc <Unit Location>
[Device-Name]>set sysctname <Contact Name (person responsible for system)>
[Device-Name]>set sysctphone <Contact Phone Number> sysctemail <Contact E-mail address>
[Device-Name]>show system
```

```
[Device Name]> show system
System Parameters
=================

sysname                  :       Device Name
sysloc                   :       System Location
sysctname                :       Contact Name
sysctemail               :       name@Organization.com
sysctphone               :       Contact Phone Number
sysuptime (DD:HH:MM:SS)  :        0:11: 6:40
sysoid                   :       1.3.6.1.4.1.11898.2.4.6
sysdescr                 :        AP v2.5.0  SN-02UT16570004 v2.5.0
sysservices              :       2
sysflashupdate           :       0
sysflashbckint           :       120
sysresettodefaults       :       0

[Device Name]> _
```

Figure A-12 Result of "show system" CLI Command

Set Static IP Address for the AP

NOTE: *The IP Subnet Mask of the AP must match your network's Subnet Mask.*

```
[Device-Name]>set ipaddrtype static
[Device-Name]>set ipaddr <fixed IP address of unit>
[Device-Name]>set ipsubmask <IP Mask>
[Device-Name]>set ipgw <gateway IP address>
[Device-Name]>show network
```

Change Passwords

```
[Device-Name]>passwd <Old Password> <New Password> <Confirm Password> (CLI password)
[Device-Name]>set httppasswd <New Password> (HTTP interface password)
[Device-Name]>set snmprpasswd <New Password> (SNMP read password)
[Device-Name]>set snmprwpasswd <New Password> (SNMP read/write)
[Device-Name]>set snmpv3authpasswd <New Password> (SNMPv3 authentication password)
[Device-Name]>set snmpv3privpasswd <New Password> (SNMPv3 privacy password)
[Device-Name]>reboot 0
```

CAUTION: *Proxim strongly urges you to change the default passwords to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the* Reset to Factory Default Procedure.

Set Network Names for the Wireless Interface

```
[Device-Name]>set wif <index 3 (Wireless Interface A) or 4 (Wireless Interface B)>
netname <Network Name (SSID) for wireless interface>
[Device-Name]>show wif
```

```
[Device Name]> show wif
Wireless Interface Table
========================


Index                          :       3
Network Name                   :       My Wireless Network A
Distance Between APs           :       large
Interference Robustness        :       disable
DTIM Period                    :       1
Automatic Channel Selection    :       enable
Frequency Channel              :       56
RTS/CTS Medium Reservation     :       2347
Multicast Rate                 :       2 MBps
Closed System                  :       disable
Load Balancing                 :       enable
Medium Density Distribution    :       disable
MAC Address                    :       00:30:F1:65:09:E9
Supported Data Rates           :       6 9 12 18 24 36 48 54
Supported Frequency Channels   :       52 56 60 64 36 40 44 48 149 153 157 161
Physical Layer Type            :       OFDM
Regulatory Domain List         :       USA (FCC)
Transmit Rate                  :       0
TurboMode                      :       disable
```

Figure A-13 Results of "show wif" CLI command for an AP

Enable 802.11d Support and Set the Country Code

Perform the following command to enable 802.11d IEEE 802.11d support for additional regulatory domains.

`[Device-Name]>set wif` **`<3 (Wireless Interface A) or 4 (Wireless Interface B)>`** `dot11dstatus <enable/disable>`

Perform the following command to set a country code:

`[Device-Name]>set syscountrycode <country code>`

Select a country code from the following table. Note that not all countries are available for all products. This table is derived from ISO 3166.

Country	Code	Country	Code	Country	Code
Algeria	DZ	Honduras	HN	Panama	PA
Albania	AL	Hong Kong	HK	Papua New Guinea	PG
Argentina	AR	Hungary	HU	Peru	PE
Armenia	AM	Iceland	IS	Philippines	PH
Australia	AU	India	IN	Poland	PL
Austria	AT	Indonesia	ID	Portugal	PT
Azerbaijan	AZ	Ireland 5.8 GHz	I1	Puerto Rico	PR
Bahrain	BH	Israel	IL	Qatar	QA
Belarus	BY	Italy	IT	Romania	RO
Belgium	BE	Jamaica	JM	Russia	RU
Belize	BZ	Japan	JP	Samoa	WS
Bolivia	BO	Japan2	J2	Saudi Arabia	SA
Brazil	BR	Jordan	JO	Singapore	SG
Brunei Darussalam	BN	Kazakhstan	KZ	Slovak Republic	SK
Bulgaria	BG	North Korea	KP	Slovenia	SI
Canada	CA	Korea Republic	KR	South Africa	ZA

Country	Code	Country	Code	Country	Code
Chile	CL	Korea Republic2	K2	South Korea	KR
China	CN	Kuwait	KW	Spain	ES
Colombia	CO	Latvia	LV	Sweden	SE
Costa Rica	CR	Lebanon	LB	Switzerland	CH
Croatia	HR	Liechtenstein	LI	Syria	SY
Cyprus	CY	Lithuania	LT	Taiwan	TW
Czech Republic	CZ	Luxembourg	LU	Thailand	TH
Denmark	DK	Macau	MO	Turkey	TR
Dominican Republic	DO	Macedonia	MK	Ukraine	UA
Ecuador	EC	Malaysia	MY	United Arab Emirates	AE
Egypt	EG	Malta	MT	United Kingdom	GB
El Salvador	SV	Mexico	MX	United Kingdom 5.8ghz	G1
Estonia	EE	Monaco	MC	United States	US
Finland	FI	Morocco	MA	United States World	UW
France	FR	Netherlands	NL	United States Dfs	U1
Georgia	GE	New Zealand	NZ	Uruguay	UY
Germany	DE	Nicaragua	NI	Venezuela	VE
Greece	GR	Norway	NO	Vietnam	VN
Guam	GU	Oman	OM		
Guatemala	GT	Pakistan	PK		

Enable and Configure TX Power Control for the Wireless Interface(s)

The TX Power Control feature lets the user configure the transmit power level of the card in the AP at one of four levels:

- 100% of the maximum transmit power level of the card
- 50%
- 25%
- 12.5%

Perform the following commands to enable TX Power Control and set the transmit power level:

```
[Device-Name]>set txpowercontrol enable


[Device-Name]>set wif <interface number> currenttxpowerlevel <value>
Allowed values are: 1 (100%), 2 (50%), 3 (25%), 4 (12.5%)
```

Configure SSIDs (Network Names), VLANs, and Profiles

Perform the following command to configure SSIDs and VLANS, and to assign Security and RADIUS Profiles.

```
[Device-Name]>set wifssidtbl <Wireless Interface Index.SSID Index> ssid <Network Name>
vlanid <-1 to 1094> ssidauth <enable/disable> acctstatus <enable/disable> secprofile
<Security Profile Nmuber> radmacprofile <MAC Authentication Profile Name> radeapprofile
<EAP Authentication Profile Name> radacctprofile <Accounting Profile Name>
radmacauthstatus <enable/disable> aclstatus <enable/disable>
```

Examples:

```
[Device-Name]>set wifssidtbl 3.1 ssid accesspt1 vlanid 22 ssidauth enable acctstatus
enable secprofile 1 radmacprofile "MAC Authentication" radeapprofile "EAP Authentication"
radacctprofile "Accounting" radmacauthstatus enable aclstatus enable

[Device-Name]>set wifssidtbl 4.1 ssid accesspt1 vlanid 22 ssidauth enable acctstatus
enable secprofile 1 radmacprofile "MAC Authentication" radeapprofile "EAP Authentication"
radacctprofile "Accounting" radmacauthstatus enable aclstatus enable
```

Download an AP Configuration File from your TFTP Server

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

```
[Device-Name]>set tftpfilename <file name> tftpfiletype config
           tftpipaddr <IP address of your TFTP server>
[Device-Name]>show tftp (to ensure the filename, file type, and the IP address are correct)
[Device-Name]>download *
[Device-Name]>reboot 0
```

After following the complete process (above) once, you can download a file of the same name (so long as all the other parameters are the same), with the following command:

```
[Device-Name]>download *
```

Backup your AP Configuration File

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

```
[Device-Name]>upload <TFTP Server IP address> <tftpfilename (such as "config.sys")> config
[Device-Name]>show tftp (to ensure the filename, file type, and the IP address are correct)
```

After setting the TFTP parameters, you can backup your current file (so long as all the other parameters are the same), with the following command:

```
[Device-Name]>upload *
```

Set up Auto Configuration

The Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Perform the following commands to enable and set up automatic configuration:

NOTE: *The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP. The default filename is "config". The default TFTP IP address is "169.254.128.133".*

```
[Device-Name]>set autoconfigstatus <enable/disable>

[Device-Name]>set autoconfigfilename <filename>
Enter the filename of the configuration file that is used if the AP is configured for
Static IP.

[Device-Name]>set autoconfigTFTPaddr <IP address>
Enter the TFTP server address that is used if the AP is configured for Static IP.
```

Other Network Settings

There are other configuration settings that you may want to set for the AP. Some of them are listed below.

- Configure the AP as a DHCP Server
- Configure the DNS Client
- Configure DHCP Relay and Configure DHCP Relay Servers
- Maintain Client Connections using Link Integrity
- Change your Wireless Interface Settings
- Set Ethernet Speed and Transmission Mode
- Set Interface Management Services
- Configure Wireless Distribution System
- Configure MAC Access Control
- Set RADIUS Parameters
- Set Rogue Scan Parameters
- Set Hardware Configuration Reset Parameters
- Set VLAN/SSID Parameters
- Set Security Profile Parameters

NOTE: *See Advanced Configuration for more information on these settings.*

Configure the AP as a DHCP Server

NOTE: *You must have at least one entry in the DHCP Server IP Address Pool Table before you can set the DHCP Server Status to Enable.*

```
[Device-Name]>set dhcpstatus disable
[Device-Name]>set dhcpippooltbl 0 startipaddr <start ip address>
            endipaddr <end ip address>
[Device-Name]>set dhcpgw <gateway ip address>
[Device-Name]>set dhcppridnsipaddr <primary dns ip address>
[Device-Name]>set dhcpsecdnsipaddr <secondary dns ip address>
[Device-Name]>set dhcpstatus enable
[Device-Name]>reboot 0
```

CAUTION: *Before enabling this feature, confirm that the IP address pools you have configured are valid addresses on the network and do not overlap the addresses assigned by any other DHCP server on the network. Enabling this feature with incorrect address pools will cause problems on your network.*

Configure the DNS Client

```
[Device-Name]>set dnsstatus enable
[Device-Name]>set dnsprisvripaddr <IP address of primary DNS server>
[Device-Name]>set dnssecsvripaddr <IP address of secondary DNS server>
[Device-Name]>set dnsdomainname <default domain name>
[Device-Name]>show dns
```

```
[Device Name]> show dns
DNS Client Group
================

dnsstatus       :       disable
dnsprisvripaddr :       0.0.0.0
dnssecsvripaddr :       0.0.0.0
dnsdomainname   :
```

Figure A-14 Results of “show dns” CLI command

Configure DHCP Relay

Perform the following command to enable or disable DHCP Relay Agent Status.

NOTE: *You must have at least one entry in the DHCP Relay Server Table before you can set the DHCP Relay Status to Enable.*

```
[Device-Name]>set dhcprelaystatus enable
```

Configure DHCP Relay Servers

Perform the following command to configure and enable a DHCP Relay Server. The AP allows the configuration of a maximum of 10 server settings in the DHCP Relay Agents server table.

```
[Device-Name]>set dhcprlyindex 1 dhcprlyipaddr <ip address> dhcprlycmt <comment>
dhcprlystatus 1 (1 to enable, 2 to disable, 3 to delete, 4 to create)
```

Maintain Client Connections using Link Integrity

```
[Device-Name]>show linkinttbl (this shows the current links)
[Device-Name]>set linkinttbl <1-5 (depending on what table row you wish to address)>
              ipaddr <ip address of the host computer you want to check>
[Device-Name]>set linkintpollint <the interval between link integrity checks>
[Device-Name]>set linkintpollretx <number of times to retransmit before considering the
link down>
[Device-Name]>set linkintstatus enable
[Device-Name]>show linkinttbl （to confirm new settings）
[Device-Name]>reboot 0
```

Change your Wireless Interface Settings

See Interfaces for information on the parameters listed below. The AP-4000/4000M/4900M uses index 3 for Wireless Interface A (802.11a radio) and index 4 for Wireless Interface B (802.11b/g radio).

Operational Mode

```
[Device-Name]>set wif <index> mode <see table>
```

Mode	Operational Mode
1	dot11b-only
2	dot11g-only
3	dot11bg
4	dot11a-only
5	dot11g-wifi
6	publicsafety

Autochannel Select (ACS)

ACS is enabled by default. Reboot after disabling or enabling ACS.

```
[Device-Name]>set wif <index> autochannel <enable/disable>
[Device-Name]>reboot 0
```

Enable/Disable Closed System

[Device-Name]>**set wif <index> closedsys <enable/disable>**

Shutdown/Resume Wireless Service

[Device-Name]>**set wif <index> wssstatus <1 (resume)/2 (shutdown)>**

Set Load Balancing Maximum Number of Clients

[Device-Name]>**set wif <index> lbmaxclients <1–63>**

Set the Multicast Rate (802.11a)

[Device-Name]>**set wif 3 multrate <6, 12, 24 (Mbits/sec)>**

Set the Multicast Rate (802.11b/g)

[Device-Name]>**set wif 4 multrate <1,2,5.5,11 (Mbits/sec)>**

Enable/Disable Super Mode (802.11a/g only)

[Device-Name]>**set wif 3 supermode <enable/disable>**

Enable/Disable Turbo Mode (802.11a/g only)

[Device-Name]>**set wif 3 turbo <enable/disable>**

NOTE: *Super mode must be enabled on the interface before Turbo mode can be enabled.*

NOTE: *Turbo mode and Mesh mode (either Mesh AP or Mesh Portal) can not be enabled on the same interface simultaneously.*

Configure Antenna Diversity

NOTE: *When the AP-4900M is configured to use the 4.9 GHz Public Safety operational mode, antenna diversity is disabled, and antenna 3 is statically configured for use. It is not configurable by the administrator. If an operational mode other than 4.9 Public Safety is configured, the administrator may manually select which antenna to use.*

[Device-Name]>**set wif 3 atdiversity <3, 4, 5(auto)>** (see below)

[Device-Name]>**set wif 4 atdiversity <1, 2, 5(auto)>** (see below)

[Device-Name]>**reboot**

Value	Corresponding Antenna Enabled
1	802.11b/g (connector 1)
2	802.11b/g (connector 2)
3	802.11a (connector 3)
4	802.11a (connector 4)
5 (auto)	Both antennas on interface

NOTE: *See* Antennas *for more information on internal and external antenna ports.*

Set the Distance Between APs

`[Device-Name]>set wif <index> distaps <1-5>` (see below)

`[Device-Name]>reboot 0`

Value	Distance Between APs
1	Large
2	Medium
3	Small
4	Mini
5	Micro

Set Ethernet Speed and Transmission Mode

```
[Device-Name]>set etherspeed <value> (see below)
[Device-Name]>reboot 0
```

Ethernet Speed and Transmission Mode	Value
10 Mbits/sec - half duplex	10halfduplex
10 Mbits/sec - full duplex	10fullduplex
10 Mbits/sec - auto duplex	10autoduplex
100 Mbits/sec - half duplex	100halfduplex
100 Mbits/sec - full duplex	100fullduplex
Auto Speed - half duplex	autohalfduplex
Auto Speed - auto duplex	autoautoduplex (default)

Set Interface Management Services

Edit Management IP Access Table

`[Device-Name]>set mgmtipaccesstbl <index> ipaddr <IP address> ipmask <subnet mask>`

Configure Management Ports

```
[Device-Name]>set snmpifbitmask <(see below)>
[Device-Name]>set httpifbitmask <(see below)>
```

[Device-Name]>**set telifbitmask <**(see below)**>**

Choose from the following values:

Interface Bitmask	Description
0 or 2 = Disable (all interfaces)	All management channels disabled
1 or 3 = Ethernet only	Ethernet only enabled
4 or 6 = Wireless A only	Wireless A only enabled
8 or 10 = Wireless B only	Wireless B only enabled
12 = Wireless A and Wireless B	Wireless A and Wireless B enabled
13 or 15 = All interfaces	All management channels enabled

Set Communication Ports

[Device-Name]>**set httpport <HTTP port number** (default is 80)**>**
[Device-Name]>**set telport <Telnet port number** (default is 23)**>**

Configure Secure Socket Layer (HTTPS)

Enabling SSL and configuring a passphrase allows encrypted Secure Socket Layer communications to the AP through the HTTPS interface.

[Device-Name]>**set sslstatus <enable/disable>**

The user must change the SSL passphrase when uploading a new certificate/private key pair, which will have a corresponding passphrase.

[Device-Name]>**set sslpassphrase <SSL certificate passphrase>**

[Device-Name]>**show http** (to view all HTTP configuration information including SSL.)

```
HTTP Group Parameters
=====================

httpifbitmask           :       15
httppasswd              :       ********
httpport                :       80
httphelplink            :       file:///C:/Program Files/ORiNOCO/AP4xxx/HTML/index.htm
httpsetupwiz            :       disable
sslstatus               :       enable
sslpassphrase           :       ********
```

Figure A-15 Result of “show HTTP” CLI Command

Set Telnet Session Timeouts

[Device-Name]>**set tellogintout <time in seconds between 1 and 300** (default is 30)**>**
[Device-Name]>**set telsessiontout <time in seconds between 1 and 36000** (default is 900)**>**

Configure Serial Port Interface

NOTE: *To avoid unexpected performance issues, leave Flow Control at the default setting (none) unless you are sure what this setting should be.*

```
[Device-Name]>set serbaudrate <2400, 4800, 9600, 19200, 38400, 57600>
[Device-Name]>set serflowctrl <none, xonxoff>
[Device-Name]>show serial
```

```
[Device Name]> show serial
Serial Interface Group Parameters
=================================

serbaudrate             :       9600
serdatabits             :       8
serparity               :       none
serstopbits             :       1
serflowctrl             :       none
```

Figure A-16 Result of "show serial" CLI Command

Configure Syslog

```
[Device-Name]>set syslogpriority <1-7 (default is 6)>
[Device-Name]>set syslogstatus <enable/disable>
[Device-Name]>set sysloghbstatus <enable/disable> (default is disable)
[Device-Name]>set sysloghbinterval <1-604800> (default is 900 seconds)
[Device-Name]>set sysloghosttbl <index> ipaddr <ipaddress> cmt <comment> status
<enable/disable>
```

Configure Intra BSS

```
[Device-Name]>set intrabssoptype <passthru (default)/block)>
```

Configure Wireless Distribution System

Create/Enable WDS

```
[Device-Name]>set wdstbl <Index> partnermacaddr <MAC Address> status enable
```

Enable/Disable WDS

```
[Device-Name]>set wdstbl <Index> status <enable/disable>
```

NOTE: **<Index>** *is 3.1–3.6 (Wireless A) or 4.1–4.6 (Wireless B). To determine the index, type show* **wdstbl** *at the prompt.*

Configure MAC Access Control

Setup MAC (Address) Access Control

```
[Device-Name]>set wifssidtbl <index> aclstatus enable/disable
[Device-Name]>set macacloptype <passthru, block>
[Device-Name]>reboot 0
```

Add an Entry to the MAC Access Control Table

```
[Device-Name]>set macacltbl 0 macaddr <MAC Address> status enable
[Device-Name]>show macacltbl
```

Disable or Delete an Entry in the MAC Access Control Table

```
[Device-Name]>set macacltbl <index> status <disable/delete>
[Device-Name]>show macacltbl
```

NOTE: *For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the RADIUS parameters (see* Set RADIUS Parameters*).*

Set RADIUS Parameters

Configure RADIUS Authentication servers

Perform the following command to configure a RADIUS Server and assign it to a VLAN. The RADIUS Server Profile index is specified by the index parameter and the subindex parameter specifies whether you are configuring a primary or secondary RADIUS server.

```
[Device-Name]>set radiustbl <Index> profname <Profile Name> seraddrfmt <1 - IP Address 2 - Name> sernameorip <IP Address or Name> port <value> ssecret <value> responsetm <value> maxretx <value> acctupdtintrvl <value> macaddrfmt <value> authlifetm <value> radaccinactivetmr <value> vlanid <vlan id -1 to 4094> status enable
```

NOTE: *To create a new RADIUS profile, use 0 for* **<Index>**.

Examples of Configuring Primary and Secondary RADIUS Servers and Displaying the RADIUS Configuration

Primary server configuration:

```
[Device-Name]set radiustbl 1.1 profname "MAC Authentication" seraddrfmt 1 sernameorip 20.0.0.20 port 1812 ssecret public responsetm 3 maxretx 3 acctupdtintrvl 0 macaddrfmt 1 authlifetm 900 radaccinactivetmr 5 vlanid 22 status enable
```

Secondary server configuration:

```
[Device-Name]set radiustbl 1.2 profname "MAC Authentication" seraddrfmt 1 sernameorip 20.0.0.30 port 1812 ssecret public responsetm 3 maxretx 3 acctupdtintrvl 0 macaddrfmt 1 authlifetm 900 radaccinactivetmr 5 vlanid 33 status enable
```

```
[Device-Name]>show radiustbl

Index                          : 1
Primary/Backup                 : Primary
Profile Name                   : MAC Authentication
Server Status                  : notReady
Server Addressing Format       : ipaddr
IP Address/Host Name           : 0.0.0.0
Destination Port               : 1812
VLAN Identifier                : -1
MAC Address Format             : dashdelimited
Response Time                  : 3
Maximum Retransmission         : 3
Authorization Lifetime         : 0
Accounting Update Interval     : 0
Accounting Inactivity Timer    : 5


Index                          : 1
Primary/Backup                 : Backup
Profile Name                   : MAC Authentication
Server Status                  : notReady
Server Addressing Format       : ipaddr
IP Address/Host Name           : 0.0.0.0
Destination Port               : 1812
VLAN Identifier                : -1
MAC Address Format             : dashdelimited
Response Time                  : 3
```

```
Maximum Retransmission          : 3
.
.
.
Index                           : 4
Primary/Backup                  : Backup
Profile Name                    : Management Access
Server Status                   : notReady
Server Addressing Format        : ipaddr
IP Address/Host Name            : 0.0.0.0
Destination Port                : 1812
VLAN Identifier                 : -1
MAC Address Format              : dashdelimited
Response Time                   : 3
Maximum Retransmission          : 3
Authorization Lifetime          : 0
Accounting Update Interval      : 0
Accounting Inactivity Timer    : 5
```

Figure A-17 Result of "showradiustbl" CLI Command

Set Rogue Scan Parameters

Perform the following command to enable or disable Rogue Scan on a wireless interface and configure the scanning parameters.

The **cycletime** parameter is only configured for background scanning mode.

[Device-Name]>**set rscantbl <3, 4> mode <1 for background scanning, 2 for continuous scanning> cycletime <cycletime from 1–1440 minutes> status <enable, disable>**

NOTE: *Rogue Scan cannot be enabled on a wireless interface when the Wireless Service Status on that interface is shutdown. First, resume service on the wireless interface.*

Set Hardware Configuration Reset Parameters

The Hardware Configuration Reset commands allows you to enable or disable the hardware reset functionality and to change the password to be used for configuration reset during boot up.

To disable hardware configuration reset, enter:

[Device-Name]>**set hwconfigresetstatus disable**

To enable hardware configuration reset, enter:

[Device-Name]>**set hwconfigresetstatus enable**

To define the Configuration Reset Password to be used for configuration reset during boot up, enter the following command

[Device-Name]>**set configresetpasswd <password>**

It is important to safely store the

NOTE: *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disable.*

Set VLAN/SSID Parameters

Enable VLAN Management

```
[Device-Name]>set vlanstatus enable
[Device-Name]>set vlanmgmtid <1-4094>
```

```
[Device-Name]>show wifssidtbl (to review your settings)
[Device-Name]>reboot 0
```

Disable VLAN Management

```
[Device-Name]>set vlanstatus disable or
[Device-Name]>set vlanmgmtid -1
[Device-Name]>reboot 0
```

Add a Entry to the WIFSSID Table

```
[Device-Name]>set wifssidtbl <index> ssid <Network Name> vlanid <-1 (untagged) or 1-4094>
status enable
```

Set Security Profile Parameters

Configure a Security Profile with Non Secure Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode nonsecure status enable
```

Example:
```
[Device-Name]>set secprofiletbl 2 secmode nonsecure status enable
```

Configure a Security Profile with WEP Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wep encryptkey0 <value> encryptkeylength
<vakue> encryptkeytx <value> status enable
```

Example:
```
[Device-Name]>set secprofiletbl 3 secmode wep encryptkey0 12345 encryptkeylength 1
encryptkeytx 0 status enable
```

Configure a Security Profile with 802.1x Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode 802.1x rekeyint 900 status enable
```

Example:
```
[Device-Name]>set secprofiletbl 4 secmode 802.1x rekeyint 900 status enable
```

Configure a Security Profile with WPA Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wpa rekeyint 900 status enable
```

Example:
```
[Device-Name]>set secprofiletbl 5 secmode wpa rekeyint 900 status enable
```

Configure a Security Profile with WPA-PSK Security Mode

```
[Device-Name]>set secprofiletbl <index> secmode wpa-psk passphrase <value> status enable
```

Example:
```
[Device-Name]>set secprofiletbl 6 secmode wpa-psk passphrase 12345678 status enable
```

Configure a Security Profile with 802.11i Security Mode

[Device-Name]>**set secprofiletbl <index> secmode 802.11i rekeyint <value> status enable**

Example:
[Device-Name]>set secprofiletbl 7 secmode 802.11i rekeyint 900 status enable

Configure a Security Profile with 802.11i-PSK Security Mode

[Device-Name]>**set secprofiletbl <index> secmode 802.11i-psk passphrase <value> status enable**

Example:
[Device-Name]>set secprofiletbl 8 secmode 802.11i-psk passphrase 12345678 status enable

CLI Monitoring Parameters

Using the **show** command with the following table parameters will display operating statistics for the AP (these are the same statistics that are described in the Monitoring section).

- **staticmp:** Displays the ICMP statistics.
- **statarptbl:** Displays the IP ARP Table statistics.
- **statbridgetbl:** Displays the Learn Table.
- **statiapp:** Displays the IAPP statistics.
- **statradius:** Displays the RADIUS Authentication statistics.
- **statif:** Displays information and statistics about the Ethernet and wireless interfaces.
- **stat802.11:** Displays additional statistics for the wireless interfaces.
- **statethernet:** Displays additional statistics for the Ethernet interface.
- **statmss:** Displays station statistics and Wireless Distribution System links.
- **statmesh**: Displays statistics about the Mesh network.

Parameter Tables

Objects contain groups that contain both parameters and parameter tables. Use the following Tables to configure the Access Point. Columns used on the tables include:

- Name - Parameter, Group, or Table Name
- Type - Data type
- Value - Value range, and default value, if any
- Access = access type, R = Read Only (show), RW = Read-Write (can be “set”), W = Write Only
- CLI Parameter - Parameter name as used in the Access Point

Access Point network objects are associated with Groups. The network objects are listed below and associated parameters are described in the following Parameter Tables:

- System Parameters - Access Point system information
  - Inventory Management Information - Hardware, firmware, and software version information
- Network Parameters - IP and Network Settings
  - IP Configuration Parameters - Configure the Access Point’s IP settings
    - DNS Client for RADIUS Name Resolution - Configure the Access Point as a DNS client
  - DHCP Server Parameters - Enable or disable dynamic host configuration
  - SNTP Parameters - Configure

  - Link Integrity Parameters - Monitor link status
- Interface Parameters - Configure Wireless and Ethernet settings
  - Wireless Interface Parameters
    - Channel Blacklist Parameters - View and configure blacklisted channels
    - Wireless Distribution System (WDS) Parameters - Configure the WDS partnerships
  - Wireless Interface SSID/VLAN/Profile Parameters - Configure the SSIDs, VLANs, and security modes for each interface. Up to 16 SSIDs per wireless interface are supported; different security settings can be applied to each SSID, and a unique VLAN can be configured per SSID.
  - Ethernet Interface Parameters - Set the speed and duplex of the Ethernet port.
  - Mesh Network Parameters - Configure the Mesh network.
- Management Parameters - Control access to the AP's management interfaces
  - SNMP Parameters - Set read and read/write passwords
  - HTTP Parameters - Set up the graphical web browser interface. If required, enable SSL and configure the SSL certificate passphrase.
  - Telnet Parameters - Telnet Port setup
  - Serial Port Parameters - Serial Port setup
  - RADIUS Based Management Access Parameters - Configure RADIUS Based Management Access for HTTP and Telnet access.
  - SSH Parameters - Enable SSH and configure the host key.
  - TFTP Server Parameters - Set up for file transfers; specify IP Address, file name, and file type
  - IP Access Table Parameters - Configure range of IP addresses that can access the AP
  - Auto Configuration Parameters - Configure the Auto Configuration feature which allows an AP to be automatically configured by downloading a configuration file from a TFTP server during boot up.
- Filtering Parameters
  - Ethernet Protocol Filtering Parameters - Control network traffic based on protocol type
  - Static MAC Address Filter Table - Enable and disable specific addresses
  - Proxy ARP Parameters - Enable or disable proxy ARP for wireless clients
  - IP ARP Filtering Parameters - Control which ARP messages are sent to wireless clients based on IP settings
  - Broadcast Filtering Table - Control the type of broadcast packets forwarded to the wireless network
  - TCP/UDP Port Filtering - Filter IP packets based on TCP/UDP port
- Alarms Parameters
  - SNMP Table Host Table Parameters - Enter the list of IP addresses that will receive alarms from the AP
  - Syslog Parameters - Configure the AP to send Syslog information to network servers
- Bridge Parameters
  - Spanning Tree Parameters - Used to help prevent network loops
  - Storm Threshold Parameters - Set threshold for number of broadcast packets
  - Intra BSS Subscriber Blocking - Enable or disable peer to peer traffic on the same AP
  - Packet Forwarding Parameters - Redirect traffic from wireless clients to a specified MAC address
- RADIUS Parameters
  - Set RADIUS Parameters - Configure RADIUS Servers and assign them to VLANs.
- Security Parameters - Access Point security settings
  - MAC Access Control Parameters - Control wireless access based on MAC address
  - Rogue Scan Configuration Table - Enable and configure Rogue Scan to detect Rogue APs and clients.
  - 802.1X Parameters - Configure 802.1X Supplicant Timeout parameter

  - Hardware Configuration Reset - Disable or enable hardware configuration reset and configure a configuration reset password.
  - Other Parameters - Configure Security Profiles that define allowed security modes (wireless clients), and encryption and authentication mechanisms.
- VLAN/SSID Parameters - Enable the configuration of multiple subnetworks based on VLAN ID and SSID.
- Other Parameters
  - IAPP Parameters - Enable or disable the Inter-Access Point Protocol
  - Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters - Enable and configure Wireless Multimedia Enhancement/Quality of Service parameters, QoS policies, mapping priorities, and EDCA parameters. Apply a configured QoS policy to a particular SSID.

System Parameters

Name	Type	Value	Access	CLI Parameter
System	Group	N/A	R	system
Name	DisplayString	User Defined	RW	sysname
Location	DisplayString	User Defined	RW	sysloc
Contact Name	DisplayString	User Defined	RW	sysctname
Contact E-mail	DisplayString	User Defined	RW	sysctemail
Contact Phone	DisplayString	User Defined max 254 characters	RW	sysctphone
FLASH Backup Interval	Integer	0 - 65535 seconds	RW	sysflashbckint
Flash Update		0 1	RW	sysflashupdate
System OID	DisplayString	N/A	R	sysoid
Descriptor	DisplayString	System Name, flash version, S/N, bootloader version	R	sysdescr
Up Time	Integer	dd:hh:mm:ss dd - days hh - hours mm - minutes ss - seconds	R	sysuptime
System Security ID	DisplayString	Retrieved from flash ID	R	sysinvmgmtsecurityid
Emergency Restore to defaults		Resets all parameters to default factory values	RW	sysresettodefaults Note: You must enter the following command twice to reset to defaults: **set sysresettodefaults 1**

Inventory Management Information

Name	Type	Value	Access	CLI Parameter
System Inventory Management	Subgroup	N/A	R	sysinvmgmt
Component Table	Subgroup	N/A	R	sysinvmgmtcmptbl
Component Interface Table	Subgroup	N/A	R	sysinvmgmtcmpiftbl

NOTE: *The inventory management commands display advanced information about the AP's installed components. You may be asked to report this information to a representative if you contact customer support.*

Network Parameters

IP Configuration Parameters

Name	Type	Value	Access	CLI Parameter
Network	Group	N/A	R	network
IP Configuration	Group	N/A	R	ip (Note: The **network** and **ip** parameters display the same information)
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Default Router IP Address	IpAddress	User Defined	RW	ipgw
Default TTL	Integer	User Defined (seconds) 0 - 255, 64 (default)	RW	ipttl
Address Type	Integer	static dynamic (default)	RW	ipaddrtype

NOTE: *The IP Address Assignment Type (ipaddrtype) must be set to static before the IP Address (ipaddr), IP Mask (ipmask) or Default Gateway IP Address (ipgw) values can be entered.*

DNS Client for RADIUS Name Resolution

Name	Type	Value	Access	CLI Parameter
DNS Client	Group	N/A	R	dns
DNS Client status	Integer	enable disable (default)	RW	dnsstatus
Primary DNS Server IP Address	IpAddress	User Defined	RW	dnspridnsipaddr
Secondary DNS Server IP Address	IpAddress	User Defined	RW	dnssecdnsipaddr
Default Domain Name	Integer32	User Defined (up to 254 characters)	RW	dnsdomainname

DHCP Server Parameters

Name	Type	Value	Access	CLI Parameter
DHCP Server	Group	N/A	R	dhcp
DHCP Server Status	Integer	enable (1) (default) disable (2) delete (3)	RW	dhcpstatus
Gateway IP Address	IpAddress	User Defined	RW	dhcpgw
Primary DNS IP Address	IpAddress	User Defined	RW	dhcppridnsipaddr
Secondary DNS IP Address	IpAddress	User Defined	RW	dhcpsecdnsipaddr
Number of IP Pool Table Entries	Integer32	N/A	R	dhcpippooltblent

NOTE: *The DHCP Server (dhcpstatus) can only be enabled after a DHCP IP Pool table entry has been created.*

DHCP Server table for IP pools

Name	Type	Value	Access	CLI Parameter
DHCP Server IP Address Pool Table	Table	N/A	R	dhcpippooltbl
Table Index	Integer	User Defined	N/A	index
Start IP Address	IpAddress	User Defined	RW	startipaddr
End IP Address	IpAddress	User Defined	RW	endipaddr
Width	Integer	User Defined	RW	width
Default Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	defleasetm
Maximum Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	maxleasetm
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

NOTE: *Set either End IP Address or Width (but not both) when creating an IP address pool.*

DHCP Relay Group

The DHCP Relay Group allows you to enable or disable DHCP Relay Agent Status.

Name	Type	Value	Access	CLI Parameter
DHCP Relay Group	Group	N/A	R	dhcprelay
Status	Integer	enable disable	RW	dhcprelaystatus
DHCP Relay Server Table	Table		R	dhcprelaytbl

DHCP Relay Server Table

The DHCP Relay Server Table contains the commands to set the table entries. The AP supports the configuration of a maximum of 10 server settings in the DHCP Relay Agents server table.

Name	Type	Value	Access	CLI Parameter
DHCP Relay Server Table	Table	N/A	R	dhcprelaytbl
DHCP Relay Server Table Entry Index	Integer32	1 - 10	R	dhcprlyindex
DHCP Relay Server Table Entry IP Address	IpAddress	User Defined	RW	dhcprlyipaddr
DHCP Relay Server Table Entry Comment	DisplayString	User Defined	RW	dhcprlycmt
DHCP Relay Server Table Entry Status	Integer	enable (1) disable (2) delete (3) create (4)	RW	dhcprlystatus

SNTP Parameters

Name	Type	Value	Access	CLI Parameter
SNTP Group	Group	N/A	R	sntp
SNTP Status	Integer	enable disable	RW	sntpstatus
Primary Server Name or IP Address	DisplayString	0 - 255 characters	RW	sntpprisvr
Secondary Server Name or IP Address	DisplayString	0 - 255 characters	RW	sntpsecsvr
Time Zone	Integer	See MIB for requirements	RW	sntptimezone
Daylight Savings Time	Integer	-2 -1 0 +1 +2	RW	sntpdaylightsaving
Year	Integer32	N/A	RW	sntpyear
Month	Integer32	1 - 12	RW	sntpmonth
Day	Integer32	1 - 31	RW	sntpday
Hour	Integer32	0 - 23	RW	sntphour
Minutes	Integer32	0 - 59	RW	sntpmins
Seconds	Integer32	0 - 59	RW	sntpsecs
Addressing Format	Integer	ipaddress name	RW	sntpaddrfmt

Link Integrity Parameters

Name	Type	Value	Access	CLI Parameter
Link Integrity*	Group	N/A	R	linkint
Link Integrity Status*	Integer	enable disable (default)	RW	linkintstatus
Link Integrity Poll Interval*	Integer	500 - 15000 ms (in increments of 500ms) 500 ms (default)	RW	linkintpollint
Link Integrity Poll Retransmissions*	Integer	0 - 255 5 (default)	RW	linkintpollretx

* Link integrity cannot be configured when the AP is configured to function as a Mesh AP.

Link Integrity IP Target Table

Name	Type	Value	Access	CLI Parameter
Link Integrity IP Target Table	Table	N/A	R	linkinttbl
Table Index	Integer	1 - 5	N/A	index
Target IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable disable (default) delete	RW	status

Interface Parameters

Wireless Interface Parameters

The wireless interface group parameter is **wif**. Wireless Interface A (802.11a radio) uses table index 3 and Wireless Interface B (802.11b/g radio) uses table index 4.

Common Parameters to 802.11a/b/g

Name	Type	Value	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Table Index	Integer	3 (Wireless Interface A) or 4 (Wireless Interface B)	R	index
Network Name	DisplayString	1 - 32 characters My Wireless Network (default)	RW	netname
Auto Channel Select (ACS)*	Integer	enable (default) disable	RW	autochannel
DTIM Period	Integer	1 - 255 1 = default	RW	dtimperiod
RTS/CTS Medium Reservation	Integer	0 - 2347 Default is 2347 (off)	RW	medres
MAC Address	PhyAddress	12 hex digits	R	macaddr
Closed System	Integer	enable disable (default)	RW	closedsys
Wireless Service Status†	Integer	1 = resume 2 = shutdown	RW	wssstatus
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Load Balancing Max Clients	Integer	1 - 63	RW	lbmaxclients
Distance Between APs‡	Integer	1 (large) (default) 2 (medium) 3 (small), 4 (minicell) 5 (microcell)	RW	distaps
Antenna Diversity§	Integer	1 (Antenna 1), 2 (Antenna 2), 3 (Antenna 3),§ 4 (Antenna 4), 5 (Auto; both antennas on radio) (See Configure Antenna Diversity)	RW	atdiversity
AP Link Length**	Integer	200 (default) - 15000	RW	aplinklength

* For 802.11a APs certified in the ETSI and TELEC regulatory domains and operating in the middle frequency band, disabling Auto Channel Select will limit the available channels to those in the lower frequency band.

† Wireless Service Status cannot be shut down on an interface where Rogue Scan is enabled.

‡ Distance Between APs allows the AP to perform better in high noise environments by increasing the recieve sensitivity and transmit defer threshold, as follows:

Distance Between APs	Receive Sensitivity Threshold		Transmit Defer Threshold	
	Value	dBm	Value	dBm
Large	0	-96	33	-62
Medium	9	-86	33	-62
Small	17	-78	43	-52

Distance Between APs	Receive Sensitivity Threshold		Transmit Defer Threshold	
	Value	dBm	Value	dBm
Mini	25	-70	53	-42
Micro	33	-62	59	-36

§ When the AP-4900M is configured to use the 4.9 GHz Public Safety operational mode, antenna diversity is disabled, and antenna 3 is statically configured for use. If an operational mode other than 4.9 Public Safety is configured, antenna diversity is configurable by the administrator.

** WDS and Mesh technologies have been designed for outdoor use. Each 802.11 packet is acknowledged by the receiving station. On links longer than about 100m, the time that it takes for the ACK to get back to the sending station is long enough to cause the sending station to believe that the packet was not properly received. This problem can be corrected by adjusting the AP Link Length parameter to a value that is larger than the length in meters of the longest link being serviced by that AP.

802.11a Only Parameters

Name	Type	Value	Access	CLI Parameter
Operating Frequency Channel	Integer	Varies by regulatory domain and country. See Available Channels	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates
Transmit Rate	Integer32	0 (Auto Fallback; default) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ofdm (orthogonal frequency division multiplexing) for 802.11a	R	phytype
Super Mode	Integer	enable disable (default)	RW	supermode
Turbo Mode*	Integer	enable disable (default)	RW	turbo

* Super mode must be enabled on the wireless interface before Turbo mode can be enabled. Turbo mode and Mesh mode (either Mesh AP or Mesh Portal) can not be enabled on the same interface simultaneously.

802.11b Only Parameters

Name	Type	Value	Access	CLI Parameter
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see Available Channels	RW	channel
Multicast Rate	Integer	1 Mbits/sec (1) 2 Mbits/sec (2) (default) 5.5 Mbits/sec (3) 11 Mbits/sec (4)	RW	multrate
Closed Wireless System	Integer	enable disable (default)	RW	closedsys
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	R	suppdatarates
Transmit Rate	Integer32	0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	RW	txrate
Physical Layer Type	Integer	dsss (direct sequence spread spectrum) for 802.11b	R	phytype
Regulatory Domain List	DisplayString	U.S./Canada -- FCC Europe -- ETSI Japan -- TELEC	R	regdomain

802.11b/g Only Parameters

Name	Type	Value	Access	CLI Parameter
Wireless Operational Mode	Integer	dot11b-only dot11g-only dot11bg (default)	RW	mode
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see Available Channels	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates

Name	Type	Value	Access	CLI Parameter
Transmit Rate	Integer32	**For 802.11b-only mode:** 0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec **For 802.11g-only mode:*** 0 (auto fallback; default) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec **For 802.11b/g mode:** 0 (auto fallback; default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ERP (Extended Rate Protocol)	R	phytype
Super Mode	Integer	enable disable (default)	RW	supermode
Turbo Mode†	Integer	enable disable (default)	RW	turbo

* Also for 802.11g-wifi mode. 802.11g-wifi has been defined for Wi-Fi testing purposes; it is not recommended for use in your wireless network environment.

† Super mode must be enabled on the wireless interface before Turbo mode can be enabled. Turbo mode and Mesh mode (either Mesh AP or Mesh Portal) can not be enabled on the same interface simultaneously.

Channel Blacklist Parameters

Name	Type	Value	Access	CLI Parameter
Wireless Interface Channel Blacklist Table	Table	wifchblklisttbl	R	wdstbl
Interface Index	Integer	Wireless interface A = 3 Wireless interface B = 4	R	ifindex
Channel Number	Integer	Depends on regulatory domain	R	channel
Radar Detected	TruthValue	True False	R	radardetected
Elapsed Time (minutes)	Gauge32	0 - 32	R	elapsetime
Blacklist Status	ObjStatus	enable disable	RW	status

Wireless Distribution System (WDS) Parameters

Name	Type	Value	Access	CLI Parameter
WDS Table	Table	N/A	R	wdstbl
Port Index	Integer	3.1 - 3.6 (Wireless)	R	portindex
Status	Integer	enable, disable	RW	status
Partner MAC Address	PhysAddress	User Defined	RW	partnermacaddr

Wireless Interface SSID/VLAN/Profile Parameters

The Wireless Interface SSID table manages the SSIDs, VLANs, Security Profiles, and RADIUS Profiles associated to each SSID.

For configuration examples, see Configure SSIDs (Network Names), VLANs, and Profiles.

Name	Type	Value	Access	CLI Parameter
Wireless Interface SSID Table	Table	N/A	R	wifssidtbl
Table Index	Integer	Primary wireless interface = 3 Secondary wireless interface = 4	R	index
Table Index	Integer32	1 - 16 (SSID index)	R	ssidindex
SSID	DisplayString	2 - 32 characters	RW	ssid
Broadcast SSID	Integer	enable disable	R/W	bcastbeaconssid
Closed System	Integer	enable, disable	R/W	denybcastprobereq
VLAN ID	VlanId	-1 - 4094 or untagged	RW	vlanid
Rekeying Interval	Integer32	0 (disabled) 300 - 65535	R/W	reykeyint
Table Row Status	RowStatus	enable disable delete	RW	status
SSID Authorization Status per VLAN	Integer	enable disable	RW	ssidauth

RADIUS Accounting Status per VLAN	Integer	enable disable	RW	acctstatus
MAC ACL Status per VLAN	Integer	enable disable	RW	aclstatus
Security Profile	Integer32	User defined	RW	secprofile
RADIUS MAC Profile	DisplayString	User defined	RW	radmacprofile
RADIUS EAP Profile	DisplayString	User defined	RW	radeapprofile
RADIUS Accounting Profile	DisplayString	User defined	RW	radacctprofile
QoS Policy	Integer32	User defined	RW	qospolicy

Wireless Distribution System (WDS) Security Table Parameters

The WDS Security Table manages WDS related security objects.

Name	Type	Value	Access	CLI Parameter
WDS Security Table	Table	N/A	R	wdssectbl
Table Index	Integer	Primary wireless interface = 3 Secondary wireless interface = 4	R	index
Security Mode	Integer	1 (none) 2 (wep)	RW	secmode
Encryption Key 0	WEPKeyType	N/A	WO	encryptkey0

Ethernet Interface Parameters

Name	Type	Value	Access	CLI Parameter
Ethernet Interface	Group	N/A	R	ethernet
Speed	Integer	1 (10halfduplex) 2 (10fullduplex) 3 (10autoduplex) 4 (100halfduplex) 5 (100fullduplex) 6 (autohalfduplex) 7 (autoautoduplex) (default)	RW	etherspeed
MAC Address	PhyAddress	N/A	R	ethermacaddr

Mesh Network Parameters

Name	Type	Value	Access	CLI Parameter
Mesh Group	Group	N/A	R	mesh
Mesh Mode	Integer	disable (default) portal ap	RW	meshmode
Mesh Interface Number	Integer32	3 (Wireless Interface A) 4 (Wireless Interface B)	RW	meshwif
Mesh SSID	DisplayString	1–16 characters	RW	meshssid
Security Mode	Integer	none aes (default)	RW	meshsecurity
Shared Secret	DisplayString	6–32 characters Default: public	W	meshssecret
Maximum Active Mesh Links	Integer32	1–6 Default: 6	RW	meshmaxlinks
RSSI Smoothing*	Integer32	4, 8, 16 (default), 32	RW	meshrssismoothing
Roaming Threshold*	Integer32	40, 60, 80 (default), 100	RW	meshroamingthreshold
Send Client Deauth Message	ObjStatus	enable (default) disable	RW	meshsenddeauth

* Higher RSSI smoothing and roaming threshold values create a more static mesh envrironment. Lower RSSI smoothing and roaming threshold values create a more dynamic mesh envrionment

Management Parameters

Secure Management Parameters

Name	Type	Value	Access	CLI Parameter
Secure Management	Integer	1 (enable) 2 (disable)	RW	securemgmtstatus

SNMP Parameters

Name	Type	Value	Access	CLI Parameter
SNMP	Group	N/A	R	snmp
SNMP Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless A 8 or 10 = Wireless B 12 = Wireless A & B 13 or 15 = All interfaces (default is 15)	RW	snmpifbitmask
Read Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmprpasswd
Read/Write Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmprwpasswd
SNMPv3 Authentication Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmpv3authpasswd

SNMPv3 Privacy Password	DisplayString	User Defined public (default) 6 - 32 characters	W	snmpv3privpasswd

HTTP Parameters

Name	Type	Value	Access	CLI Parameter
HTTP	Group	N/A	R	http
HTTP Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless A 8 or 10 = Wireless B 12 = Wireless A & B 13 or 15 = All interfaces (default is 15)	RW	httpifbitmask
HTTP Password	DisplayString	User Defined (6 - 32 characters)	W	httppasswd
HTTP Port	Integer	User Defined Default = 80	RW	httpport
Help Link*	DisplayString	User Defined	RW	httphelplink
SSL Status	Integer	enable/disable	RW	sslstatus
SSL Certificate Passphrase	DisplayString	User Defined	W	sslpassphrase

* The help link must be set to an HTTP address. Use the forward slash character ("/") rather than the backslash character ("\") when configuring the Help Link location.

Telnet Parameters

Name	Type	Value	Access	CLI Parameter
Telnet	Group	N/A	R	telnet
Telnet Management Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless A 8 or 10 = Wireless B 12 = Wireless A & B 13 or 15 = All interfaces (default is 15)	RW	telifbitmask
Telnet Port	Integer	User Defined 23 (default)	RW	telport
Telnet Login Inactivity Time-out	Integer	30 - 300 seconds 60 sec (default)	RW	tellogintout
Telnet Session Idle Time-out	Integer	60 - 36000 seconds 900 sec (default)	RW	telsessiontout

Serial Port Parameters

Name	Type	Value	Access	CLI Parameter
Serial	Group	N/A	R	serial
Baud Rate	Integer	2400, 4800,9600 (default), 19200, 38400, 57600	RW	serbaudrate
Data Bits	Integer	8	R	serdatabits
Parity	Integer	none	R	serparity
Stop Bits	Integer	1	R	serstopbits
Flow Control	Value	none (default) xonxoff	RW	serflowctrl

RADIUS Based Management Access Parameters

The RADIUS Based Management Access parameters allow you to enable HTTP or Telnet Radius Management Access, enable or disable local user access, and configure the local user password.

The default local user ID is root and the default local user password is public. “Root” cannot be configured as a valid user for RADIUS based management access when local user access is enabled.

Name	Type	Value	Access	CLI Parameter
Radius Local User Status	Integer	enable disable	RW	radlocaluserstatus
Radius Local User Password	DisplayString	User Defined	RW	radlocaluserpasswd
HTTP Radius Management Access	Integer	enable disable	RW	httpradiusmgmtaccess
Telnet Radius Management Access	Integer	enable disable	RW	telradiusmgmtaccess

SSH Parameters

The following commands enable or disable SSH and set the SSH host key.

Name	Type	Value	Access	CLI Parameter
SSH Status	Integer	enable disable	RW	sshstatus
SSH Public Host Key Fingerprint	DisplayString	AP Generated	RW	sshkeyfprint
SSH Host Key Status	Integer	create delete	RW	sshkeystatus

The AP SSH feature, open-SSH, confirms to the SSH protocol, and supports SSH version 2. The following SSH clients have been verified to interoperate with the AP’s server. The following table lists the clients, version number, and the website of the client.

Clients	Version	Website
OpenSSH	V3.4-2	http://www.openssh.com
Putty	Rel 0.53b	http://www.chiark.greenend.org.uk
Zoc	5.00	http://www.emtec.com
Axessh	V2.5	http://www.labf.com

For key generation, only the OpenSSH client has been verified.

Auto Configuration Parameters

These parameters relate to the Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Name	Type	Value	Access	CLI Parameter
Auto Configuration	Group	N/A	R	autoconfig
Auto Configuration Status	Integer	enable (default) disable	RW	autoconfigstatus
Auto Config File Name	DisplayString	User Defined	RW	autoconfigfilename
Auto Config TFTP Server IP Address	IpAddress	User Defined	RW	autoconfigTFTPaddr

TFTP Server Parameters

These parameters relate to upload and download commands.

When a user executes an upload and/or download Command, the specified arguments are stored in TFTP parameters for future use. If nothing is specified in the command line when issuing subsequent upload and/or download commands, the stored arguments are used.

Name	Type	Value	Access	CLI Parameter
TFTP	Group	N/A	R	tftp
TFTP Server IP Address	IpAddress	User Defined	RW	tftpipaddr
TFTP File Name	DisplayString	User Defined	RW	tftpfilename
TFTP File Type	Integer	img config bootloader sslcertificate sslprivatekey sshprivatekey sshpublickey clibatchfile (CLI Batch File) cbflog (CLI Batch Error Log)	RW	tftpfiletype

IP Access Table Parameters

When creating table entries, you may either specify the argument name followed by argument value or simply entering the argument value. When only the argument value is specified, then enter the values in the order depicted by the following table. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Value	Access	CLI Parameter
IP Access Table	Table	N/A	R	mgmtipaccesstbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Filtering Parameters

Ethernet Protocol Filtering Parameters

Name	Type	Value	Access	CLI Parameter
Ethernet Filtering	Group	N/A	R	etherflt
Filtering Interface Bitmask	Interface Bitmask	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless A 8 or 10 = Wireless B 12 = Wireless A & B 13 or 15 = All interfaces (default is 15)	RW	etherfltifbitmask
Operation Type		passthru block	RW	etherfltoptype

Ethernet Filtering Table

Identify the different filters by using the table index.

Name	Type	Value	Access	CLI Parameter
Ethernet Filtering Table	Table	N/A	R	etherflttbl
Table Index	N/A	N/A	R	index
Protocol Number	Octet String	N/A	RW	protonumber
Protocol Name (optional)	DisplayString		RW	protoname
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

NOTE: *The filter Operation Type (passthru or block) applies* ***only*** *to the protocol filters that are* ***enabled*** *in this table.*

Static MAC Address Filter Table

Name	Type	Value	Access	CLI Parameter
Static MAC Address Filter Table	Table	N/A	R	staticmactbl
Table Index	N/A	N/A	R	index
Static MAC Address on Wired Network	PhysAddress	User Defined	RW	wiredmacaddr
Static MAC Address Mask on Wired Network	PhysAddress	User Defined	RW	wiredmask
Static MAC Address on Wireless Network	PhysAddress	User Defined	RW	wirelessmacaddr
Static MAC Address Mask on Wireless Network	PhysAddress	User Defined	RW	wirelessmask
Comment (optional)	DisplayString	max 255 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Proxy ARP Parameters

Name	Type	Value	Access	CLI Parameter
Proxy ARP	Group	N/A	R	parp
Status	Integer	enable disable (default)	RW	parpstatus

IP ARP Filtering Parameters

Name	Type	Value	Access	CLI Parameter
IP ARP Filtering	Group	N/A	R	iparp
Status	Integer	enable disable (default)	RW	iparpfltstatus
IP Address	IpAddress	User Defined	RW	iparpfltipaddr
Subnet Mask	IpAddress	User Defined	RW	iparpfltsubmask

Broadcast Filtering Table

Name	Type	Value	Access	CLI Parameter
Broadcast Filtering Table	Table	N/A	R	broadcastflttbl
Index	Integer	1 - 5	N/A	index
Protocol Name	DisplayString	N/A	R	protoname
Direction	Integer	ethertowireless wirelesstoether both (default)	RW	direction
Status	Integer	enable disable (default)	RW	status

TCP/UDP Port Filtering

The following parameters are used to enable/disable the Port filter feature.

Name	Type	Value	Access	CLI Parameter
Port Filtering	Group	N/A	R	portflt
Port Filter Status	Integer	enable (default) disable	RW	portfltstatus

TCP/UDP Port Filtering Table

The following parameters are used to configure TCP/UDP Port filters.

Name	Type	Value	Access	CLI Parameter
Port Filtering Table	Table	N/A	R	portflttbl
Table Index	N/A	User Defined (there are also 4 pre-defined indices, see Port Number below for more information)	R	index
Port Type	Octet String	tcp udp tcp/udp	RW	porttype

Name	Type	Value	Access	CLI Parameter
Port Number	Octet String	User Defined (there are also 4 pre-defined protocols: Index 1: NetBios Name Service - 137, Index 2: NetBios Datagram Service - 138, Index 3: NetBios Session Service - 139, Index 4: SNMP Service - 161)	RW	portnum
Protocol Name	DisplayString	User Defined (there are also 4 pre-defined protocols, see Port Number above)	RW	protoname
Interface Bitmask	Integer32	0 or 2 = No interfaces (disable) 1 or 3 = Ethernet 4 or 6 = Wireless A 8 or 10 = Wireless B 12 = Wireless A & B 13 or 15 = All interfaces (default is 15)	RW	ifbitmask
Status (optional)	Integer	enable (default for new entries) disable (default for pre-defined entries) delete	RW	status

Alarms Parameters

SNMP Table Host Table Parameters

When creating table entries, you may either specifying the argument name followed by argument value. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Value	Access	CLI Parameter
SNMP Trap Host Table	Table	N/A	R	snmptraphosttbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Password	DisplayString	User Defined (up to 64 characters)	W	passwd
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Syslog Parameters

The following parameters configure the Syslog settings.

Name	Type	Value	Access	CLI Parameter
Syslog	Group	N/A	R	syslog
Syslog Status	Integer	enable disable (default)	RW	syslogstatus
Syslog Port	Octet String	514	R	syslogport
Syslog Lowest Priority Logged	Integer	1 - 7 1 = LOG_ALERT 2 = LOG_CRIT 3 = LOG_ERR 4 = LOG_WARNING 5 = LOG_NOTICE 6 = LOG_INFO (default) 7 = LOG_DEBUG	RW	syslogpritolog
Heartbeat Status	Integer	enable (1) disable (2) (default)	RW	sysloghbstatus
Heartbeat Interval (seconds)	Integer	1 - 604800 seconds; 900 sec. (default)	RW	sysloghbinterval

NOTE: *When Heartbeat is enabled, the AP periodically sends a message to the Syslog server to indicate that it is active. The frequency with which the heartbeat message is sent depends upon the setting of the Heartbeat Interval.*

Syslog Host Table

The table described below configures the Syslog hosts that will receive message from the AP. You can configure up to ten Syslog hosts.

Name	Type	Value	Access	CLI Parameter
Syslog Host Table	Table	N/A	R	sysloghosttbl
Table Index	Integer	1 - 10	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Bridge Parameters

Spanning Tree Parameters

Name	Type	Value	Access	CLI Parameter
Spanning Tree	Group	N/A	R	stp
Spanning Tree Status	Integer	enable (default) disable	RW	stpstatus
Bridge Priority	Integer	0 - 65535 32768 (default)	RW	stppriority
Maximum Age	Integer	600 - 4000 (in 0.01 sec intervals; i.e., 6 to 40 seconds) 2000 (default)	RW	stpmaxage
Hello Time	Integer	100 - 1000 (1/100 second; i.e., 1 to 10 seconds); enter values in increments of 100 200 (default)	RW	stphellotime
Forward Delay	Integer	400 - 3000 (in 0.01 sec intervals; i.e., 4 to 30 seconds) 1500 (default)	RW	stpfwddelay

Spanning Tree Priority and Path Cost Table

Name	Type	Value	Access	CLI Parameter
Spanning Tree Table	Table	N/A	R	stpbl
Table Index (Port)	N/A	1 - 15	R	index
Priority	Integer	0 - 255 128 (default)	RW	priority
Path Cost	Integer	1 - 65535 100 (default)	RW	pathcost
State	Integer	disable blocking listening learning forwarding broken	R	state
Status	Integer	enable disable	RW	status

Storm Threshold Parameters

Name	Type	Value	Access	CLI Parameter
Storm Threshold	Group	N/A	N/A	stmthres
Broadcast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	stmbrdthres
Multicast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	stmmultithres

Storm Threshold Table

Name	Type	Value	Access	CLI Parameter
Storm Threshold Table	Table	N/A	R	stmthrestbl
Table Index	Integer	1 = Ethernet 3 = Wireless	R	index
Broadcast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	bcast
Multicast Threshold	Integer	0 - 255 packets/sec (default is 0)	RW	mcast

Intra BSS Subscriber Blocking

The following parameters control the Intra BSS traffic feature, which prevent wireless clients that are associated with the same AP from communicating with each other:

Name	Type	Value	Access	CLI Parameter
Intra BSS Traffic	Group	N/A	R	intrabss
Intra BSS Traffic Operation	Integer	passthru (default) block	RW	intrabssoptype

Packet Forwarding Parameters

The following parameters control the Packet Forwarding feature, which redirects wireless traffic to a specific MAC address:

Name	Type	Value	Access	CLI Parameter
Packet Forwarding MAC Address	Group	N/A	R	pktfwd
Packet Forwarding MAC Address	MacAddress	User Defined	RW	pktfwdmacaddr
Packet Forwarding Status	Integer	enable disable (default)	RW	pktfwdstatus
Packet Forwarding Interface Port	Integer	0 (any) (default) 1 (Ethernet) 2 (WDS 1) 3 (WDS 2) 4 (WDS 3) 5 (WDS 4) 6 (WDS 5) 7 (WDS 6)	RW	pktfwdif

RADIUS Parameters

General RADIUS Parameters

Name	Type	Value	Access	CLI Parameter
RADIUS	Group	N/A	R	radius
Client Invalid Server Address	Counter32	N/A	R	radcliinvsvradd

RADIUS Server Configuration Parameters

NOTE: *Use a server name only if you have enabled the DNS Client functionality. See* DNS Client for RADIUS Name Resolution*.*

Name	Type	Value	Access	CLI Parameter
RADIUS Authentication	Table	N/A	R	radiustbl
Table Index (Profile Index)	Integer	N/A	R	index
Primary/Secondary Index	Integer	Primary (1) Secondary (2)	R	subindex
Status	Integer	enable disable	RW	status
Server Address Format	Integer	Ipaddr Name	RW	seraddrfmt
Server IP Address or Name	IpAddress DisplayString	User defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name; up to 254 characters if using a name)	RW	ipaddr
Port (optional)	Integer	User Defined 1812 (default)	RW	port
Shared Secret	DisplayString	User Defined 6 - 32 characters	W	ssecret
Response Time (optional)	Integer	1 - 10 seconds 3 (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	0 - 4 3 (default)	RW	maxretx
RADIUS MAC Address Format	Integer	dashdelimited colondelimited singledashdelimited nodelimiter	RW	radmacaddrformat
RADIUS Accounting Inactivity Timer	Integer32	1 - 60 minutes	RW	radaccinactivetmr
Authorization Lifetime	Integer32	900 - 43200 seconds	W	radauthlifetm
RADIUS Accounting Update Interval	Integer32	10 - 3600 minutes	RW	radacctupdinterval
VLAN ID	vlanID	-1 (untagged) 1 - 4094	RW	radvlanid

Security Parameters

MAC Access Control Parameters

Name	Type	Value	Access	CLI Parameter
MAC Address Control	Group	N/A	R	macacl
Status	Integer	enable disable (default)	RW	aclstatus
Operation Type	Integer	passthru (default) block	RW	macacloptype

MAC Access Control Table

Name	Type	Value	Access	CLI Parameter
MAC Address Control Table	Table	N/A	R	macacltbl
Table Index	N/A	N/A	R	index
MAC Address	PhysAddress	User Defined	RW	macaddr
Comment (optional)	DisplayString	User Defined max 254 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Rogue Scan Configuration Table

The Rogue Scan Configuration Table allows you to enable or disable Rogue Scan and configure the scanning parameters.

Name	Type	Value	Access	CLI Parameter
Rogue Scan Configuration Table	Table	N/A	R	rscantbl
Rogue Scan Mode	Integer	Bkscan (1) Contscan (2)	RW	mode
Rogue Scan Cycle Time	Integer	1 - 1440	RW	cycletime
Rogue Scan Configuration Table Index	Integer	3 or 4	RW	index
Rogue Scan Status	Integer	enable disable	RW	status

802.1X Parameters

Name	Type	Value	Access	CLI Parameter
802.1X Group	Group	N/A	R	dot1xauthcfg
802.1X Supplicant Timeout	Integer32	3 - 60 seconds	RW	dot1xsupptimeout

Hardware Configuration Reset

The Hardware Configuration Reset commands allows you to enable or disable the feature and to change the password to be used for configuration reset during boot up.

Name	Type	Value	Access	CLI Parameter
Hardware Configuration Reset Status	Integer	enable (1) disable (2)	R	hwconfigresetstatus
Configuration Reset Password	DisplayString	User Defined	RW	configresetpasswd

Security Profile Table

The Security Profile Table allows you to configure security profiles. A maximum of 16 security profiles are supported per wireless interface.

Each security profile can be enable and configure one or more security modes (None Secure Station, WEP Station, 802.1x Station, WPA Station, WPA-PSK Station). The WEP/PSK parameters are separately configurable for each security mode. See the command examples below for more information.

Name	Type	Value	Access	CLI Parameter
Security Profile Table	Table	N/A	R	secprofiletbl
Table Index	Integer	1.1 to 32.5	R	index
Security Mode	Integer	nonsecsta wepsta 802.1xsta wpasta wpapsksta	R	secmode
Authentication Mode	Integer	none 802.1x psk	R	authmode
Cipher	Integer	none wep tkip aes	R	ciphersuite
Encryption Key 0	Integer	User defined	W	encryptionkey0
Encryption Key 1	Integer	User defined	W	encryptionkey1
Encryption Key 2	Integer	User defined	W	encryptionkey2
Encryption Key 3	Integer	User defined	W	encryptionkey3
Encryption Transmit Key	Integer	0 - 3	RW	encryptkeytx
Encryption Key Length	Integer	64, 128, or 152	RW	encryptkeylength
Rekey Interval	Integer		RW	rekeyint
WPA PSK Value	Integer		W	pskkey
WPA PSK Pass Phrase	Integer	8 - 64 characters	W	passphrase

VLAN/SSID Parameters

Name	Type	Value	Access	CLI Parameter
VLAN	Group	N/A	R	vlan
Status	Integer	enable disable (default)	RW	vlanstatus
Management ID	VlanId	-1 (untagged) or 1 - 4094	RW	vlanmgmtid

Other Parameters

IAPP Parameters

Name	Type	Value	Access	CLI Parameter
IAPP	Group	N/A	R	iapp
IAPP Status	Integer	enable (default) disable	RW	iappstatus
Periodic Announce Interval (seconds)	Integer	80 120 (default) 160 200	RW	iappannint
Announce Response Time	Integer	2 seconds	R	iappannresp
Handover Time-out	Integer	410 ms 512 ms (default) 614 ms 717 ms 819 ms	RW	iapphandtout
Max. Handover Retransmissions	Integer	1 - 4 (default 4)	RW	iapphandretx
Send Announce Request on Startup	Integer	enable (default) disable	RW	iappannreqstart

NOTE: *These parameters configure the Inter Access Point Protocol (IAPP) for roaming. Leave these settings at their default value unless a technical representative asks you to change them.*

Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters

The Wireless Multimedia Enhancements commands enable and configure Wireless Multimedia Enhancement/Quality of Service parameters per wireless interface. The following two commands are part of the Wireless Interface Properties table.

Enabling QoS

Name	Type	Value	Access	CLI Parameter
QoS Status	Object Status	enable disable (default)	RW	qosstatus
QoS Maximum Medium Threshold	Integer	50 - 90	RW	qosmaximummediumthreshold

Configuring QoS Policies

The QoS group manages the QoS policies:

Name	Type	Value	Access	CLI Parameter
QoS Group	Group	N/A	N/A	qos
QoS Policy Table	Table	N/A	N/A	qospolicytbl
Table Primary Index	Integer	N/A	R	index
Table Secondary Index	Integer	N/A	R	secindex
Policy Name	Display String	0 - 32 characters	RW	policyname
Policy Type	Integer	inlayer2, inlayer3, outlayer2, outlayer3, spectralink*	RW	type
Priority Mapping Index†	Integer	See Note†.	RW	mapindex
Apply QoS Marking	Object Status	enable disable	RW	markstatus
Table Row Status	Row Status	enable disable delete	RW	status

* QoS must be enabled on a wireless interface before spectralink can be enabled.

† A priority mapping needs to be specified for a QoS Policy. The priority mapping depends on the type of policy configured. For Layer 2 policy types (inbound or outbound) a mapping index from the 802.1p to 802.1D table should be specified. For Layer 3 policy types (inbound or outbound) a mapping index from the IP DSCP to 802.1D table should be specified. The mapping index, in both cases, depends on the number of mappings configured by the user. For SpectraLink policy type a mapping is not required.

Specifying the Mapping between 802.1p and 802.1D Priorities

The QoS 802.1p to 802.1D Mapping Table specifies the mapping between 802.1P and 802.1D priorities.

Name	Type	Value	Access	CLI Parameter
QoS 802.1p to 802.1D Mapping Table	Table	N/A	N/A	qos1pto1dtbl
Table Index (Primary Index)	Integer	0 - 7	R	index
802.1D Priority (Secondary Index)	Integer	0 - 7	R	1dpriority
802.1p Priority	Integer	0 - 7	RW	1ppriority
Table Row Status	Row Status	enable disable delete	RW	status

Specifying the Mapping between IP Precedence/DSCP Ranges and 802.1D Priorities

The QoS IP DSCP to 802.1D Mapping Table specifies the mapping between IP Precedence/DSCP Ranges and 802.1D priorities.

Name	Type	Value	Access	CLI Parameter
QoS IP DSCP to 802.1D Mapping Table	Table	N/A	N/A	qosdscpto1dtbl
Table Index (Primary Index)	Integer	0 - 7	R	index
802.1D Priority	Integer	0 - 7	R	1dpriority
IP DSCP Lower Limit	Integer	0 - 62	RW	dscplower
IP DSCP Upper Limit	Integer	1 - 63	RW	dscpupper
Table Row Status	Row Status	enable disable delete	RW	status

QoS Enhanced Distributed Channel Access (EDCA) Parameters

The following commands configure the client (STA) and AP Enhanced Distributed Channel Access (EDCA) parameters. You can modify the EDCA values for both Wireless A and Wireless B.

The EDCA parameter set provides information needed by the client stations for proper QoS operation during the wireless contention period. These parameters are used by the QoS enabled AP to establish policy, to change policies when accepting new stations or new traffic, or to adapt to changes in the offered load. The EDCA parameters assign priorities to traffic types where higher priority packets gain access to the wireless medium more frequently than lower priority packets.

NOTE: *We have defined default recommended values for EDCA parameters; we recommend not modifying EDCA parameters unless strictly necessary.*

Name	Type	Value	Access	CLI Parameter
EDCA Table	Table	N/A	N/A	qosedcatbl
Table Index	Integer	1 - 4	R	index
CWmin	Integer	0 - 255	RW	cwmin
CWmax	Integer	0 - 65535	RW	cwmax
AIFSN	Integer	2 - 15	RW	aifsn
Tx OP Limit	Integer	0 - 65535	RW	txoplimit
MSDU Lifetime	Integer	0 - 500	RW	msdulifetime
AC Mandatory	Truth Value	true false	RW	acmandatory
QAP EDCA Table	Table	N/A	N/A	qosqapedcatbl
Table Index	Integer	1 - 4	R	index
CWmin	Integer	0 - 255	RW	cwmin
CWmax	Integer	0 - 65535	RW	cwmax
AIFSN	Integer	2 - 15	RW	aifsn
Tx OP Limit	Integer	0 - 65535	RW	txoplimit
MSDU Lifetime	Integer	0 - 500	RW	msdulifetime
AC Mandatory	Truth Value	true false	RW	acmandatory

Defining the QoS Policy used for a Wireless Interface SSID

The QoS Policy object configures the QoS policy to be used per wireless interface SSID. This object is part of the Wireless Interface SSID Table; the CLI command for this table is "wifssidtbl."

Name	Type	Value	Access	CLI Parameter
QoS Policy	Integer	See Note*	RW	qospolicy

* A QoS Policy number needs to be specified in the SSID table. This depends on the QoS policies configured by the user. Once the user has configured QoS policies, the user should specify the policy to be used for that SSID.

CLI Batch File

A CLI Batch file is a user-editable file that lists a series of CLI set commands, that can be uploaded to the Access Point to change its configuration. The Access Point executes the CLI commands specified in the CLI Batch file after upload and the configuration gets changed accordingly. A CLI Batch file can also be used for Auto Configuration.

The CLI Batch file does not replace the existing LTV format configuration file, which continues to define the configuration of the AP.

The CLI Batch file contains a list of CLI commands that the AP will execute. The AP performs the commands in the file immediately after the file is uploaded to the AP manually or during Auto Configuration. The AP parses the file and executes the CLI commands. Commands that do not require a reboot take effect immediately, while commands that require a reboot (typically commands affecting a wireless interface) will take effect after reboot.

Auto Configuration and the CLI Batch File

The Auto Configuration feature allows download of the LTV format configuration file or the CLI Batch file. The AP detects whether the file uploaded is LTV format or a CLI Batch file. If the AP detects a CLI Batch file (a file with extension .cli), the AP executes the file immediately.

The AP will reboot after executing the CLI Batch file. Auto Configuration will not result in repeated reboots if the CLI Batch file contains rebootable parameters.

CLI Batch File Format and Syntax

The CLI Batch file must be named with a .cli extension to be recognized by the AP. The maximum file size allowed is 100 Kbytes, and files with larger sizes cannot be uploaded to the AP. The CLI commands supported in the CLI Batch File are a subset of the legal AP CLI commands.

The follow commands are supported:

- Set commands
- Reboot command (the reboot command ignores the argument (time))

Each command must be separated by a new line.

NOTE: *The following commands are not supported: Show command, Debug command, Undebug command, Upload command, Download command, Passwd command, Kill command, and the Exit, Quit, and Done commands.*

Sample CLI Batch File

The following is a sample CLI Batch File:

```
set sysname system1
set sysloc sunnyvale
set sysctname contact1
set sysctphone 1234567890
set sysctemail email@domain.com
```

```
set ipaddr 11.0.0.66
set ipaddrtype static
set ipsubmask 255.255.255.0
set ipgw 11.0.0.1
set wif 4 autochannel disable
set wif 4 mode 1
set syslogstatus enable
set sysloghbstatus enable
set sysloghbinterval 5
set wif 4 netname london
reboot
```

Figure A-18 Sample CLI Batch File

Reboot Behavior

When a CLI Batch file contains a reboot command, the reboot will occur only after the entire CLI Batch file has been executed.

There are two methods of uploading the CLI Batch File:

- Upload
- Upload and reboot (this option is to be used for a CLI Batch file containing the configuration parameters that require a reboot)

CLI Batch File Error Log

If there is any error during the execution of the CLI Batch file, the AP will stop executing the file. The AP generates traps for all errors and each trap contains the following information:

- Start of execution
- Original filename of the uploaded file
- End of execution (along with the status of execution)
- Line number and description of failures that occurred during execution

The AP logs all the errors during execution and stores them in the Flash memory in a CLI Batch File Error Log named “CBFERR.LOG”. The CLI Batch File Error Log can be downloaded though TFTP, HTTP, or CLI file transfer to a specified host.

B

ASCII Character Chart

You can configure WEP Encryption Keys in either Hexadecimal or ASCII format. Hexadecimal digits are 0-9 and A-F (not case sensitive). ASCII characters are 0-9, A-F, a-f (case sensitive), and punctuation marks. Each ASCII character corresponds to two hexadecimal digits.

The table below lists the ASCII characters that you can use to configure WEP Encryption Keys. It also lists the Hexadecimal equivalent for each ASCII character.

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

C

Specifications

- Software Features
- Hardware Specifications
- Available Channels

Software Features

The tables below list the software features available on the AP-4000 Series.

- Number of Stations per BSS
- Management Functions
- Advanced Bridging Functions
- Medium Access Control (MAC) Functions
- Security Functions
- Network Functions

Number of Stations per BSS

Feature	Supported by AP-4000 Series
Without encryption	up to 63
With WEP encryption	up to 63
With 802.1x Authentication	up to 63
With WPA	up to 27
With 802.11i (WPA2)	up to 63

Management Functions

Feature	Supported by AP-4000 Series
Web User Interface	✓
Telnet / CLI	✓
SNMP Agent	✓
Serial CLI	✓
Secure Management	✓
SSH	✓
RADIUS Based Management Access	✓

Advanced Bridging Functions

Feature	Supported by AP-4000 Series
IEEE 802.1d Bridging	✓
WDS Relay	✓
Roaming	✓
Protocol Filtering	✓
Multicast/Broadcast Storm Filtering	✓
Proxy ARP	✓
TCP/UDP Port Filtering	✓
Blocking Intra BSS Clients	✓
Packet Forwarding	✓

Medium Access Control (MAC) Functions

Feature	Supported by AP-4000 Series
Automatic Channel Selection (ACS)	✓
Dynamic Frequency Selection (DFS)*	✓
Closed System Feature	✓
Wireless Service Shutdown	✓
802.11d Support	✓
TX Power Control	✓
Wireless Multimedia Enhancements/Quality of Service (QoS)	✓

* DFS is required for 802.11a APs certified in the ETSI and TELEC regulatory domains and operating in the middle frequency band. When ACS is disabled, available channels are limited to those in the lower frequency band. See Dynamic Frequency Selection/Radar Detection (DFS/RD).

Security Functions

Feature	Supported by AP-4000 Series
Security Profiles per VLAN	✓
RADIUS Profiles per VLAN	✓
IEEE 802.11 WEP*	✓
MAC Access Control	✓
RADIUS MAC-based Access Control	✓
IEEE 802.1x Authentication†	✓
Multiple Authentication Server Support per VLAN‡	✓
Rogue Scanning to Detect Rogue Access Points and Clients	✓
Per User Per Session (PUPS) Encryption §	✓
Wi-Fi Protected Access (WPA)	✓
Hardware Configuration Reset Disable	✓

* Key lengths supported by 802.11a: 64-bit, 128-bit, and 152-bit.
Key lengths supported by 802.11b: 64-bit and 128-bit.
Key lengths supported by 802.11b/g: 64-bit, 128-bit, and 152-bit.

† EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP client supplicant supported.

‡ Support is provided for a primary and backup RADIUS authentication server for both MAC-based authentication and 802.1x authentication per VLAN.

§ Use in conjunction with WPA or 802.1x Authentication.

Network Functions

Feature	Supported by AP-4000 Series
DHCP Client	✓†
DHCP Server	✓
DHCP Relay Agent and IP Lease Renewal	✓†
Inter Access Point Protocol (IAPP)	✓
Link Integrity	✓
System Logging (Syslog)	✓
RADIUS Accounting Support*	✓
DNS Client	✓
TCP/IP Protocol Support	✓
Virtual LAN Support	Up to 16 SSIDs and VLANs per wireless interface, with specific Security and RADIUS profiles. For more information, see the Advanced Configuration chapter.
Mesh Networking	✓‡

* Includes Fallback to Primary RADIUS Server, RADIUS Session Timeout, RADIUS Multiple MAC Address Formats, RADIUS DNS Host Name Support, RADIUS Start/Stop Accounting.

† DHCP client requests and IP lease renewals are sent on the Ethernet interface only, not on Mesh links.

‡ Available on AP-4000M and AP-4900M only.

Hardware Specifications

Physical Specifications

Dimensions (H x W x L) = 6.5 x 18.5 x 26 cm (2.5 x 7.25 x 10.25 in.)
Weight = 1.75 Kg (3.5 lb.)

Electrical Specifications

Voltage = 100 to 240 VAC (50-60 Hz)
Current = 0.2 amp
Power Consumption = <9 Watts (power supply)

Environmental Specifications

Operating = 0°C to 55°C (32°F to 131°F) @ 5 to 95% relative humidity, non-condensing at 5°C and 55°C
Storage = -20°C to 85°C (-4°F to 185°F) @ 5 to 95% relative humidity, non-condensing at 5°C and 85°C

Ethernet Interface

10/100 Base-TX, RJ-45 female socket

Serial Port Interface

Standard RS-232C interface with DB-9, female connector

Active Ethernet Interface

Category 5, foiled, twisted pair cables must be used to ensure compliance with FCC Part 15, subpart B, Class B requirements

Standard 802.3af pin assignments

Available Channels

Available channels vary based on radio, country, and frequency band. To verify which channels are available for your product:

1. Locate the product SKU on the underside of your AP unit or on the unit's box.
2. Note the alphanumeric code following the number 8670. (e.g., 8670-**EU**)
3. See the following tables.

NOTE: *Country restrictions may apply. Please see* Regulatory Compliance*.*

AP-4000/4000M Channels

Radio	Frequency Band	Channel	Product SKU														
			AU	AU2	BR	CN	EU	EU2	HK	JP	JP2	SG	SK	TW	UK	US	US2
802.11b/g	**—**	1	✓		✓		✓			✓	✓					✓	
		2	✓		✓		✓			✓	✓					✓	
		3	✓*		✓*		✓*			✓*	✓*					✓*	
		4	✓		✓		✓			✓	✓					✓	
		5	✓		✓		✓			✓	✓					✓	
		6	✓		✓		✓			✓	✓					✓	
		7	✓		✓		✓			✓	✓					✓	
		8	✓		✓		✓			✓	✓					✓	
		9	✓		✓		✓			✓	✓					✓	
		10	✓		✓		✓			✓	✓					✓	
		11	✓		✓		✓			✓	✓					✓	
		12			✓		✓			✓	✓						
		13			✓		✓			✓	✓						
		14								✓†	✓†						
802.11a	**Lower**	34								✓*							
		36	✓	✓	✓		✓*	✓*			✓*				✓*		✓
		38								✓							
		40	✓	✓	✓		✓	✓			✓				✓		✓
		42								✓							
		44	✓	✓	✓		✓	✓			✓				✓		✓
		46								✓							
		48	✓	✓	✓		✓	✓			✓				✓		✓
	Middle	52	✓*	✓*				✓			✓				✓	✓*	✓*
		56	✓	✓				✓			✓			✓*	✓	✓	✓
		58															
		60	✓	✓				✓			✓			✓	✓	✓	✓
		64	✓	✓				✓			✓			✓	✓	✓	✓
	Upper	149	✓	✓	✓	✓*			✓*			✓*	✓*	✓		✓	✓
		153	✓	✓	✓	✓			✓			✓	✓	✓		✓	✓
		157	✓	✓	✓	✓			✓			✓	✓	✓		✓	✓
		161	✓	✓	✓	✓			✓			✓	✓	✓		✓	✓
	ISM Band	165	✓	✓	✓							✓		✓		✓	✓

* Default channel for radio.

† Available for use only in 802.11b mode.

AP-4900M Channels

Channel availability in the AP-4900M depends on the operational mode. When operating in 802.11a-only, 802.11b-only, or 802.11b/g operational mode, the AP uses the channels in the following table. Additionally, when the AP-4900M's 802.11a radio is operating in 4.9 GHz Public Safety operational mode, the AP uses channels detailed in AP-4900M Channels (4.9 GHz Public Safety Mode).

AP-4900M Channels (a/b/g Modes)

Radio	Frequency Band	Channel	Available for use in 802.11a, 802.11b, or 802.11b/g modes
802.11b/g	**—**	1	✓
		2	✓
		3	✓*
		4	✓
		5	✓
		6	✓
		7	✓
		8	✓
		9	✓
		10	✓
		11	✓
		12	
		13	
		14	
802.11a	**Lower**	34	
		36	
		38	
		40	
		42	
		44	
		46	
		48	
	Middle	52	✓*
		56	✓
		58	
		60	✓
		64	✓
	Upper	149	✓
		153	✓
		157	✓
		161	✓
	ISM Band	165	✓

AP-4900M Channels (4.9 GHz Public Safety Mode)

When operating in 4.9 GHz mode, channel availability depends on the selected frequency band.

Channel	Frequency Band	
	10 MHz	**20 MHz**
10	✓	
15		
20	✓	✓

Channel	Frequency Band	
	10 MHz	**20 MHz**
25		
30	✓	✓
35		
40	✓	✓
45		
50	✓	✓
55		
60	✓	✓
65		
70	✓	✓
75		
80	✓	✓
85		
90	✓	

D

Technical Support

If you are having a problem using an AP and cannot resolve it with the information in Troubleshooting, gather the following information and contact your local reseller:

- List of ORiNOCO products installed on your network; include the following:
  - Product names and quantity
  - Part numbers (P/N)
  - Serial numbers (S/N)
- List of ORiNOCO software versions installed
  - Check the HTTP interface's Version tab (click on **Monitor** > **Version**).
  - Include the source of the software version (e.g., pre-loaded on unit, installed from CD, downloaded from Proxim Web site, etc.)
- Information about your network
  - Network operating system (e.g., Microsoft Networking); include version information
  - Protocols used by network (e.g., TCP/IP, NetBEUI, IPX/SPX, AppleTalk)
  - Ethernet frame type (e.g., 802.3, Ethernet II), if known
  - IP addressing scheme (include address range and whether static or DHCP)
  - Network speed and duplex (10 or 100 Mbits/sec; full or half duplex)
  - Type of Ethernet device that the Access Points are connected to (e.g., Active Ethernet power injector, hub, switch, etc.)
  - Type of Security enabled on the wireless network (None, WEP Encryption, 802.1x, Mixed)
- Information about AP configuration:
  - Read/write password
- A description of the problem you are experiencing
  - What were you doing when the error occurred?
  - What error message did you see?
  - Can you reproduce the problem?
  - For each ORiNOCO product, describe the behavior of the device's LEDs when the problem occurs

If the local reseller is unable to resolve your issue, contact ORiNOCO Technical Support online or by phone, as described below.

Online Support

Software and Documentation Downloads

The latest software and documentation is available for download at http://support.proxim.com (Knowledgebase Answer ID 1250**).**

Knowledgebase

We store all resolved problems in our solution database. Search by product, category, keywords, or phrases. Also find links to drivers, documents and other downloads. Search the Knowledgebase at: <http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_alp.php>.

Submit a Knowledgebase question or open an issue at: <http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php>. Our technical support staff will reply to you by email.

NOTE: *The Knowledgebase is available to all website visitors. First-time users will be asked to create an account to gain access.*

Telephone Support

Contact technical support by phone 24 hours a day, seven days a week.

- **Domestic:** +1-866-674-6626
- **International:** 408-542-5390

E

Statement of Warranty

Warranty Coverage

Proxim Corporation warrants that its Products are manufactured solely from new parts, conform substantially to specifications, and will be free of defects in material and workmanship for a Warranty Period of **1 year** from the date of purchase.

Repair or Replacement

In the event a Product fails to perform in accordance with its specification during the Warranty Period, Proxim offers return-to-factory repair or replacement, with a thirty (30) business-day turnaround from the date of receipt of the defective Product at a Proxim Corporation Repair Center. When Proxim has reasonably determined that a returned Product is defective and is still under Warranty, Proxim shall, at its option, either: (a) repair the defective Product; (b) replace the defective Product with a refurbished Product that is equivalent to the original; or (c) where repair or replacement cannot be accomplished, refund the price paid for the defective Product. The Warranty Period for repaired or replacement Products shall be ninety (90) days or the remainder of the original Warranty Period, whichever is longer. This constitutes Buyer's sole and exclusive remedy and Proxim's sole and exclusive liability under this Warranty.

Limitations of Warranty

The express warranties set forth in this Agreement will not apply to defects in a Product caused; (i) through no fault of Proxim during shipment to or from Buyer, (ii) by the use of software other than that provided with or installed in the Product, (iii) by the use or operation of the Product in an application or environment other than that intended or recommended by Proxim, (iv) by modifications, alterations, or repairs made to the Product by any party other than Proxim or Proxim's authorized repair partners, (v) by the Product being subjected to unusual physical or electrical stress, or (vii) by failure of Buyer to comply with any of the return procedures specified in this Statement of Warranty.

Support Procedures

Buyer should return defective LAN Products[1] within the first 30 days to the merchant from which the Products were purchased. Buyer can contact a Proxim Customer Service Center either by telephone or via web. Calls for support for Products that are near the end of their warranty period should be made not longer than seven (7) days after expiration of warranty. Repair of Products that are out of warranty will be subject to a repair fee. Contact information is shown below. Additional support information can be found at Proxim's web site at http://support.proxim.com.

- LAN Products[1]: Domestic calls: 866-674-6626 (24 hours per day, 7 days per week)
- International calls: 408-542-5390
- WAN Products[2]: Domestic calls: 800-674-6626 (8:00 A.M. – 5:00 P.M, M-F Pacific Time)
- International calls: 408-542-5390

When contacting the Customer Service for support, Buyer should be prepared to provide the Product description and serial number and a description of the problem. The serial number should be on the product.

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the Product to Proxim for repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization ("RMA") number and shipping instructions. Buyer must return the defective Product to Proxim, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

1 LAN products include: ORiNOCO
2 WAN products include: Lynx, Tsunami, Tsunami MP, Tsunami Quickbridge

Calls to the Customer Service Center for reasons other than Product failure will not be accepted unless Buyer has purchased a Proxim Service Contract or the call is made within the first thirty (30) days of the Product's invoice date. Calls that are outside of the 30-day free support time will be charged a fee of $25.00 (US Dollars) per Support Call.

If Proxim reasonably determines that a returned Product is not defective or is not covered by the terms of this Warranty, Buyer shall be charged a service charge and return shipping charges.

Other Information

Search Knowledgebase

Proxim stores all resolved problems in a solution database at the following URL: http://support.proxim.com.

Ask a Question or Open an Issue

Submit a question or open an issue to Proxim technical support staff at the following URL: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php.

Other Adapter Cards

Proxim does not support internal mini-PCI devices that are built into laptop computers, even if identified as "ORiNOCO" devices. Customers having such devices should contact the laptop vendor's technical support for assistance.

For support for a PCMCIA card carrying a brand name other than Proxim, ORiNOCO, Lucent, Wavelan, or Skyline, Customer should contact the brand vendor's technical support for assistance.

F

Regulatory Compliance

NOTE: *Please read this section before installing and using your product, and save these instructions. Visit* http://support.proxim.com *for the latest regulatory compliance information.*

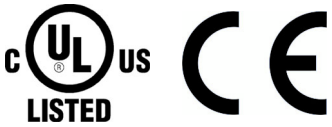
This section contains important regulatory compliance information and details for the following products:

Product	Model Numbers
ORiNOCO Tri-Mode Access Point AP-4000	AP-AG-AT-02 8670-AU 8670-AU2 8670-BR 8670-CN 8670-EU 8670-EU2 8670-HK 8670-JP 8670-JP2 8670-SG 8670-SK 8670-TW 8670-UK 8670-US 8670-US2
ORiNOCO Tri-Mode Access Point AP-4000M	AP-AG-AT-02 8670M-AU 8670M-AU2 8670M-BR 8670M-CN 8670M-EU 8670M-EU2 8670M-HK 8670M-JP 8670M-JP2 8670M-SG 8670M-SK 8670M-TW 8670M-UK 8670M-US 8670M-US2
ORiNOCO Tri-Mode Access Point AP-4900M	8670-PS

Please see the following sections for more information:

- Safety Information (USA, Canada, & European Union)
- Federal Communications Commission (FCC) (AP-4000/4000M)
- Industry Canada (IC) (AP-4000/4000M only)
- European Union (AP-4000/4000M only)
- Regulatory Compliance Certifications Summary (AP-4000/4000M)
- Regulatory Compliance Certifications Summary (AP-4900M)

Safety Information (USA, Canada, & European Union)



This product has been evaluated to, and complies with, the Safety requirements of UL60950:2000, and IEC60950:1999; the Standards for the Safety of Information Technology Equipment. When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- This product is for indoor use only.
- Operate and install this product as described in this manual. This device must be installed and used in strict accordance with the manufacturer's instructions.
- This product is suitable for installation in air handling spaces (plenum).
- Use only the AC/DC power supply adapter provided. For replacement, contact your local supplier or distributor.
- To avoid the risk of electric shock from lightning, do not use this product during an electrical storm.
- Installation of this product must conform to local regulations and codes.
- When using this product with an external antenna, see the installation documentation provided with the antenna system.
- No user serviceable parts; all repairs and service must be handled by a qualified service center.

Federal Communications Commission (FCC) (AP-4000/4000M)

DECLARATION OF CONFORMITY

This device is in conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Supplier Information	
Trade Name:	Proxim
Model:	8670-XXX
Responsible Party:	Proxim Corporation
Address:	935 Stewart Drive Sunnyvale, CA 94085
Contact Person/Title:	Mohammad Sa-id Regulatory Compliance Manager
Telephone:	(408) 542-5357
Fax:	(408) 720-9380

EUT Certification Summary	
Equipment Class:	Class B
Product Type:	ORiNOCO AP-4000 Tri-Mode Access Point
Report Number:	RF921107R02
Report Issuance Date:	2004-02-09
Tested by:	Advance Data Technology Corporation

We, the responsible party:

Proxim Corporation

declare that the product

ORiNOCO AP-4000 Tri-Mode Access Point

was tested to conform to the applicable FCC Rules and regulations. The method of testing was in accordance to the most accurate measurement standards possible, and that all necessary steps have been enforced to assure that all production units of the same equipment will continue to comply with the Federal Communications Commission's requirements.

Signature

March 1, 2004
Date

Dave Koberstein

VP, Product Marketing

Warnings

This equipment generates, uses, and can radiate radio frequency energy; and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the distance between the equipment and the receiver
- Connect the equipment to an AC outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. These situations may, for example, include the use of wireless equipment on board airplanes, or in any other environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies on the use of wireless equipment in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use this device prior to turning on the equipment.

Caution: Exposure to Radio Frequency Radiation

To comply with the FCC radio frequency exposure requirements, the following antenna installation and device operating configurations must be satisfied:

- For client devices using an integral antenna, the separation distance between the antenna(s) and any person's body (including hands, wrists, feet and ankles) must be at least 2.5 cm (1 inch).
- For Base Stations and configurations using an approved external antenna, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20 cm (8 inch).
- The transmitter shall not be collocated with other transmitters or antennas.

Modifications

The FCC requires the user to be notified that any changes or modifications to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The correction of interference caused by unauthorized modification, substitution or attachment will be the responsibility of the user. The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

Industry Canada (IC) (AP-4000/4000M only)

Industry Canada Industrie Canada

DECLARATION OF CONFORMITY

This device is in conformance with ICES-003 of the IC Rules and Regulations for Information Technology Equipment. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Supplier Information	
Trade Name:	Proxim
Model:	8670-XXX
Responsible Party:	Proxim Corporation
Address:	935 Stewart Drive Sunnyvale, CA 94085
Contact Person/Title:	Mohammad Sa-id Regulatory Compliance Manager
Telephone:	408-542-5357
Fax:	408-720-9380

EUT Certification Summary	
Equipment Class:	Class B
Product Type:	ORiNOCO AP-4000 Tri-Mode Access Point
Report Number:	RF921107R02
Report Issuance Date:	2004-02-09
Tested by:	Advance Data Technology Corporation

We, the responsible party:

Proxim Corporation

declare that the product

ORiNOCO AP-4000 Tri-Mode Access Point

was tested to conform to the applicable IC Rules and Regulations. The method of testing was in accordance to the most accurate measurement standards possible, and that all necessary steps have been in forced to assure that all production units of the same equipment will continue to comply with the Industry Canada's requirements.

Signature

March 1, 2004
Date

Dave Koberstein

VP, Product Marketing

European Union (AP-4000/4000M only)

NOTE: *European Union includes the following countries: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom; DoC also applies to Iceland, Liechtenstein, Norway, and Switzerland.*

CE1313①

DECLARATION OF CONFORMITY

July 27, 2004

We, **Proxim Corp.**

Located at, **935 Stewart Dr.**
Sunnyvale, CA 94085

Declare under our sole responsibility that the following products,

ORiNOCO AP-4000 Tri-Mode Access Point
Models AP-AG-AT-02 & 8670-XXX

Are in conformity with the following Standards and Directives,

Safety:
IEC60950:1999; EN 60950-1:2001
Immunity:
EN 55022:1994+A1:1995+A2:1997,Class B; EN 61000-3-2:2000, Class A;
EN 61000-3-3:1995+A1:2001; EN 61000-4-2:1995+A1:1998+A2:2000;
EN 61000-4-3:1995+A1:1998+A2:2000; EN 61000-4-4:1995+A1:2000;
EN 61000-4-5:1995+A1:2000; EN 61000-4-6:1996+A1:2000; EN 61000-4-11:1994+A1:2000
EMC:
EN 301-489-1 (2002-08); EN 301-489-17 (2002-08)
Radio:
EN 300 328-1 (2001-12); EN 300 328-2 (2001-12); EN 301 893 v1.2.3 (2003-08)
Directives:
European Directive 1999/5/EC, the Radio and Telecommunications Terminal Equipment Directive; Low Voltage Directive 73/23/EEC; and the Electromagnetic Compatibility Directive 89/336/EEC

Issued by: Proxim Corporation
Sunnyvale, California
July 2004

Dave Koberstein
VP, Product Marketing

Regulatory Compliance Certifications Summary (AP-4000/4000M)

Country	Certification/Reference No.
Australia & New Zealand	N11394
Brazil	ANATEL Cert. No.: 1121-04-1641
Canada	IC Cert. No.: 4110A-APAGAT02 Safety: UL File No. E177793
China	CMII ID: 2004DJ0340
European Union*	CE1313! Safety: CB Lic. No. DK-7318
India	Pending
Japan	Radio Cert. Nos.: 003NY04006 0801 003GZ04003 0801 003WY04003 0801
Mexico	COFETEL Cert. No.: RCPPR8605-039
Saudi Arabia	Pending
Singapore	IDA TAC No.: PMREQ-T1000-2004
South Korea	Radio Cert. No.: R-LARN-04-0010
Taiwan	DGT cert. No.: 93LP0049
United Arab Emirates	Pending
USA	FCC ID: IXMAPAGAT02 Safety: UL File No. E177793

* European Union includes the following countries: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom; also applies to Iceland, Liechtenstein, Norway, and Switzerland.

Regulatory Compliance Certifications Summary (AP-4900M)

Country	Certification/Reference No.
USA	FCC ID: Pending Safety: UL File No. E177793